Научная статья **https://doi.org/10.21202/2782-2923.2024.4.936-953**
УДК / UDC 004.056:343:61

А. А. Шутова[1]

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

Обеспечение цифровой безопасности системы здравоохранения уголовно-правовыми средствами

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: shutovaaa@ieml.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: GOG-9089-2022
eLIBRARY SPIN-код: 5235-4319

Аннотация

Цель: формирование теоретической концепции уголовно-правовой охраны цифрового здравоохранения на основе выявления ключевых криминальных рисков, а также терминологический анализ понятия «цифровая безопасность системы здравоохранения» и возможность его использования в юридической теории и практике.

Методы: в статье используются всеобщий диалектический метод познания, а также общенаучные (анализ, синтез, индукция, дедукция) и частнонаучные методы исследования (формально-юридический).

Результаты: на основании проведенного исследования были выявлены ключевые криминальные риски и тенденции цифрового здравоохранения, проведен юридико-терминологический анализ понятия «цифровая безопасность системы здравоохранения», сформулированы авторские определения понятий «цифровая безопасность системы здравоохранения», «обеспечение цифровой безопасности системы здравоохранения» и «цифровая угроза», а также раскрыт комплекс причин, обуславливающих необходимость правового регулирования цифровой безопасности системы здравоохранения уголовно-правовыми средствами.

Научная новизна: разработана теоретическая концепция уголовно-правовой охраны цифровой безопасности системы здравоохранения, которая включает в себя три группы элементов: ключевые криминальные риски цифровизации здравоохранения (риски, возникающие в связи с обращением цифровой информации в системе здравоохранения; риски, свойственные медицинским изделиям, разработанным на основе цифровых технологий; риски критической информационной инфраструктуры РФ); юридико-терминологический аппарат цифровой безопасности системы здравоохранения; факторы, обуславливающие необходимость правового регулирования цифровой безопасности системы здравоохранения уголовно-правовыми средствами (цифровизация здравоохранения; риски взлома или несанкционированного доступа к медицинским изделиям, созданным на основе цифровых технологий; загруженность медицинских работников; повышенная общественная опасность противоправных посягательств в сфере цифрового здравоохранения и др.).

Практическая значимость: предложения и выводы исследования могут быть использованы для совершенствования уголовного законодательства и практики его применения, а также формирования научной основы для междисциплинарных исследований на стыке уголовно-правовой науки и цифровых технологий.

Ключевые слова:

уголовно-правовые науки, уголовно-правовые средства, цифровые технологии, цифровая безопасность, система здравоохранения, медицина, робототехника

Как цитировать статью: Шутова, А. А. (2024). Обеспечение цифровой безопасности системы здравоохранения уголовно-правовыми средствами. *Russian Journal of Economics and Law*, *18*(4), 936–953. https://doi.org/10.21202/2782-2923.2024.4.936-953

Scientific article

A. A. Shutova[1]

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

Providing digital security of healthcare system with criminal-legal means

Albina A. Shutova, Cand. Sci. (Law), Senior Researcher of Scientific-research Institute for Digital Technologies and Law, Associate Professor of the Department of Criminal Law and Procedure, Kazan Innovative University named after V. G. Timiryasov
E-mail: shutovaaa@ieml.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: GOG-9089-2022
eLIBRARY SPIN-code: 5235-4319

Abstract

Objective: to form a theoretical concept of criminal-legal protection of digital healthcare by identifying the key criminal risks; to perform a terminological analysis of the concept of "digital security of the healthcare system" and to analyze the possibility of its use in legal theory and practice.

Methods: the article uses the universal dialectical method of cognition, as well as general scientific (analysis, synthesis, induction, deduction) and specific scientific (formal-legal) methods of research.

Results: based on the conducted research, the key criminal risks and trends of digital healthcare were identified; legal and terminological analysis of the concept of "digital security of the healthcare system" was performed. The author has formulates the definitions of such concepts as "digital security of the healthcare system", "ensuring digital security of the healthcare system" and "digital threat", and reveals a set of reasons for legal regulation of digital security of the healthcare system.

Scientific novelty: the author has developed a theoretical concept of criminal-legal protection of digital security of the healthcare system, which includes three groups of elements: key criminal risks in healthcare digitalization (risks arising in the circulation of digital information in the healthcare system; risks inherent in medical devices based on digital technologies; risks of critical information infrastructure in the Russian Federation); legal and terminological apparatus of digital security of the healthcare system; factors that determine the need for legal regulation of digital security of the healthcare system by criminal-legal means (digitalization of healthcare; risks of hacking or unauthorized access to medical devices based on digital technologies; workload of medical workers; increased social danger of unlawful encroachments in the field of digital healthcare, etc.).

Practical significance: the proposals and conclusions of the study can be used to improve criminal legislation and practice of its application, as well as to form a scientific basis for interdisciplinary research at the intersection of criminal law science and digital technologies.

Keywords:

criminal-legal sciences, criminal-legal means, digital technologies, digital security, healthcare system, medicine, robotics

For citation: Shutova, A. A. (2024). Providing digital security of healthcare system with criminal-legal means. *Russian Journal of Economics and Law*, *18*(4), 989–1006. (In Russ.). 936-953. https://doi.org/10.21202/2782-2923.2024.4.936-953

Введение

Повседневная деятельность человека с неизбежностью предполагает взаимодействие со всевозможными цифровыми технологиями, которые стремительно меняют представление о реальности. Специалисты уже рассматривают и выделяют цифровое право как комплексную отрасль права[1]. Активная цифровизация затронула все без исключения сферы общественной жизни, не оставив без внимания и здравоохранение. Уже сейчас активно внедряются медицинские роботы и иные автономные системы, оснащенные технологиями искусственного интеллекта, призванные качественно изменить медицину, подняв ее на новый уровень.

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. Так, распоряжением Правительства Российской Федерации от 17 апреля 2024 г. № 959-р определено стратегическое направление в области цифровой трансформации здравоохранения[2].

По причине того, что многие медицинские услуги, оказываемые населению, уходят в дистанционный режим, возрастают роль и количество цифровых данных (в том числе персональных данных) в свете внедрения методов машинного обучения и других технологий, а также в связи с тем, что здравоохранение представляет собой отрасль критической информационной инфраструктуры, непрерывность ее работы имеет большое значение для граждан страны, противоправные посягательства на цифровую составляющую учреждений здравоохранения неминуемо приведут к значимому ущербу. Таким образом, вопросам обеспечения цифровой безопасности системы здравоохранения должно уделяться пристальное внимание.

В связи с форсированной цифровизацией системы здравоохранения государству необходимо обеспечивать уровень ее безопасности в подобных условиях развития общественных отношений от нарастающих угроз (Шутова, 2023). В условиях сформированной цифровизации особенно актуальными являются вопросы обеспечения безопасности цифровых технологий (Жарова, 2023).

Развитие цифровых технологий не только трансформирует социальные связи, экономические отношения, способы взаимодействия между людьми, иные стороны общественной жизни, в том числе отрасль здравоохранения, но и провоцирует рост преступности, использование указанных инновационных решений в преступной деятельности. Злоумышленники быстро взяли на вооружение новые цифровые технологии и переместили часть своей противоправной деятельности в онлайн-пространство, вследствие чего преступность изменилась.

В связи с тем, что статистика по цифровым преступлениям в России не собирается централизованно, а в отдельных случаях кажется разрозненной, нами используются значительные сводки преступлений в других странах, так как спектр цифровых технологий, который используется в учреждениях системы здравоохранения, является схожим. Полагаем, что нам не следует дожидаться громких новостей о прорыве защиты учреждений здравоохранения Российской Федерации, а заблаговременно подготовить фундамент для формирования нормативной базы, адекватной формирующимся реалиям.

О росте цифровой преступности косвенно свидетельствуют статистические данные, сведения, полученные в результате опросов, а также исследований экспертных мнений. Имеются сведения МВД России об общем количестве совершаемых цифровых уголовно наказуемых деяний, а также данные о посягательствах на медицинские учреждения, что также позволит сделать умозаключение об их росте:

[1] Сидоренко, Э. Л. (ред.) (2024). Цифровое право: учебник. Москва: Юрлитинформ.

[2] Распоряжение Правительства Российской Федерации № 959-р от 17 апреля 2024 г. (2024). СПС «КонсультантПлюс».

1) в первом полугодии 2024 г. центр мониторинга и реагирования на кибератаки МТС *RED*, входящий в ПАО «Мобильные ТелеСистемы» (МТС), отразил на 32 % больше критических атак на эту отрасль, чем за аналогичный период прошлого года[3];

2) специалисты отдела анализа и оценки цифровых угроз ООО «Инфосекьюрити» (*Infosecurity*, входит в ГК *Softline*) подтверждают, что сфера здравоохранения в 2024 г. стала более приоритетной целью, чем в аналогичный период годом раньше[4]. В свою очередь, эксперты *KnowBe4* отмечают, что количество хакерских атак на медицинские организации значительно увеличилось, особенно во время пандемии *COVID*-19. В 2022 г. было зафиксировано увеличение атак на 45 % по сравнению с предыдущим годом, а в 2023 г. этот показатель вырос еще на 50 % по сравнению с 2021 г.[5];

3) с 2016 г. сфера здравоохранения стала жертвой большего количества атак кибербезопасности по сравнению с финансовой отраслью (Argaw et al., 2020). По результатам проведенных исследований, последствия противоправных посягательств в период пандемии коронавируса оказали сильнейшее влияние на два сектора: здравоохранение и банковскую сферу (Alawida et al., 2022);

4) согласно статистике МВД России, в январе – декабре 2023 г. зарегистрировано 677,0 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 29,7 % больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 26,5 % в январе – декабре 2022 г. до 34,8 %[6]. Однако хотелось бы уточнить, что преступления в сфере компьютерной информации, входящие в 28-ю главу УК РФ, представляют лишь часть уголовно наказуемых деяний против цифровой безопасности системы здравоохранения.

С учетом форсированной цифровизации системы здравоохранения стоит констатировать несовершенство действующего законодательства в данной области, что негативным образом влияет на охрану общественных отношений и в целом снижает потенциал предупредительных мер. По мнению профессора А. Ю. Чупровой, если «в 1996 году УК РФ справлялся с поставленными задачами по уголовно-правовой охране наиболее важных общественных отношений, то в условиях глобализации и непрерывного развития научно-технического прогресса возникновение новых видов общественных отношений представляется неизбежным» (Чупрова, 2015). Кроме этого, в российском уголовном законодательстве в настоящее время объект уголовно-правовой охраны не соответствует динамичному развитию информационных технологий (Пучков, 2022). В связи с этим приходится констатировать то, что «уголовный закон нередко отстает от существующих реалий и тенденций развития технологий. Зачастую проходят годы, прежде чем будут приняты нормы, запрещающие очевидно опасные для общества действия, или изменено законодательство» (Чупрова, 2015). Несомненно, количество уголовно-правовых норм, направленных на обеспечение информационной безопасности, в УК РФ увеличивается, что обусловлено ростом преступности, однако подобные факты не учитывают современные цифровые тенденции, а также вызовы и угрозы, которые несут подобные явления (Ефремова, 2018). В связи с этим процессы криминализации цифрового здравоохранения неизбежны, и если уже сейчас не предпринять меры предупреждения глобализации криминализации сферы, то будет значительно труднее противодействовать подобным уголовно наказуемым деяниям.

Цифровизация здравоохранения: основные тренды и проблемы практического применения

На данный момент в сфере цифрового здравоохранения наметились следующие тенденции:

– *во-первых*, в учреждениях системы здравоохранения активно применяются цифровые технологии (начиная от мобильных медицинских приложений и программного обеспечения, поддерживающих при-

[3] Хакеры взялись за медицину. (2024, 29 июля). Comnews. https://www.comnews.ru/content/234514/2024-07-29/2024-w31/1008/khakery-vzyalis-za-medicinu

[4] Там же.

[5] Хакерские атаки на сферу здравоохранения. (2023, 20 октября). Региональные системы. Инжиниринговый центр. https://www.ec-rs.ru/blog/novosti/khakerskie-ataki-na-sferu-zdravookhraneniya/

[6] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года. (2024, 20 января). МВД России. https://xn--b1aew.xn--p1ai/reports/item/47055751/

нятие клинических решений, которые врачи осуществляют каждый день, и до искусственного интеллекта и машинного обучения (Ткаченко, Чеснюкова, 2023) и их потенциал будет только расти. Технологии медицинской робототехники, искусственного интеллекта и иные инновационные медицинские решения активно используются в современной клинической медицине (Ядав, 2023) и имеют ошеломляющий успех в связи с их многочисленными преимуществами (Бахтеев, 2023). Возможности применения цифровых технологий в сфере здравоохранения разнообразны и могут быть связаны с различными инновациями, ориентированными на пациентов, например, записью на прием к врачу из дома, проверкой списков ожидания; доступом к медицинской помощи не выходя из дома, обменом информацией с другими людьми с такими же проблемами со здоровьем и доступом к персонализированной медицинской информации (Martínez-Caro et al., 2013). Цифровое здравоохранение потенциально способно предотвращать заболевания и тем самым снижать затраты на предоставляемые населению медицинские услуги, одновременно помогая пациентам контролировать, точно диагностировать и лечить хронические заболевания, а также адаптировать лекарственные средства для конкретных больных граждан (в рамках персонализированной медицинской помощи);

– *во-вторых*, увеличиваются расходы на цифровую медицину. Так, по оценкам *Statista*, расходы на цифровую трансформацию в секторе здравоохранения во всем мире уже превысили 1,3 трлн долл. и растут на 10,4 % ежегодно[7]. В свою очередь, в России также наблюдается увеличение затрат организаций на создание, распространение и использование цифровых технологий. Так, согласно данным Федеральной службы государственной статистики, в 2020 г. расходы на цифровое здравоохранение составляли 2,2 %, а в 2021 г. – 2,6 %[8], и представляется, что данные показатели будут только расти;

– *в-третьих*, медицинские работники (целых 92 %) и медицинские учреждения добились повышения производительности только за счет цифровой трансформации (согласно исследованию, опубликованному *Deloitte*)[9]. В свою очередь, журнал *The Lancet Digital Health* опубликовал результаты исследования влияния цифровых технологий на медицинских работников, в ходе которого выяснилось, что внедрение телемедицины повышает их удовлетворенность профессией и даже способствует карьерному росту (Borges do Nascimento et al. 2023);

– *в-четвертых*, цифровое здравоохранение уходит от разработки цифровых продуктов для медицинских организаций и ориентируется на пациентов. Если ранее технологические инновационные решения разрабатывались для учреждений системы здравоохранения (системы электронных карт, система поддержки принятия решений, диагностическое оборудование и т. д.), то теперь можно наблюдать тренд на разработку цифровых продуктов пациентам[10].

Таким образом, в здравоохранении традиционные методы диагностики постепенно вытесняются цифровыми методами, что привело к тому, что почти каждый компонент медицинской сферы находится в процессе оцифровки. Именно в этой сфере системообразующие элементы цифровой экономики находят свое прямое применение. Так, объем инвестиций в цифровое здравоохранение увеличивается[11].

Цифровизация системы здравоохранения породила этические, технические и правовые проблемы.

К этическим дилеммам можно отнести:

– проблему коммодификации тела человека в свете развития технологии биопринтинга;

– необходимость беречь свое здоровье в связи с возможностью замены больного органа на биопринтный, а следовательно, на здоровый. Как считает Vijayavenkataraman с соавторами, теперь можно выкурить сколько угодно сигар, а потом купить новую пару легких, напиться и купить печень в магазине органов (2016);

– использование достижений медицинской робототехники в целях оказания медицинской помощи (медицинской услуги) или трансформации тела человека и многие другие.

---

[7] Номинальный ВВП, обусловленный цифровыми и другими преобразованиями предприятий по всему миру с 2018 по 2023 гг. (2022, 23 мая). Statista. https://www.statista.com/statistics/1134766/nominal-gdp-driven-by-digitally-transformed-enterprises/

[8] Абдрахманова, Г. И., Васильковский, С. А., Вишневский, К. О. и др. (2023). Цифровая экономика: 2023: краткий статистический сборник. Москва: НИУ ВШЭ.

[9] How digital transformation is driving action in healthcare. (2022, September 9). Weforum. https://www.weforum.org/agenda/2022/09/health-information-system-digital-transformation-healthcare

[10] Тренды в цифровой медицине. (2023, 7 февраля). ProКачество https://kachestvo.pro/innovatsii/trendy-v-tsifrovoy-meditsine-/

[11] Обзор российских инвестиций в цифровое здравоохранение. (2024, 16 июля). Webiomed. https://webiomed.ru/blog/obzor-rossiiskikh-investitsii-v-tsifrovoe-zdravookhranenie/

Технические проблемы связаны с тем, что, по мнению множества специалистов по безопасности, зрелость отрасли в отношении цифровой безопасности и защиты от цифровых угроз остается довольно низкой[12]. Только 4–7 % бюджета систем здравоохранения инвестируется в их кибербезопасность (Morgan, 2020). Результаты исследования, проведенного специалистами по кибербезопасности компании «СёрчИнформ», свидетельствуют о том, что почти две трети медицинских организаций сталкивались с незаконными действиями, которые повлекли утечку данных. Кроме того, не всегда учреждения обращаются в правоохранительные органы, присутствует высокая латентность. По мнению экспертов, подобная проблема связана с нехваткой квалифицированных кадров и слабой цифровой грамотностью медицинского персонала[13]. Именно поэтому стоит констатировать отставание системы здравоохранения в обеспечении безопасности информации от иных сфер[14]. Поэтому злоумышленникам не требуются большие финансовые или ресурсные вложения для посягательства на отрасль.

В настоящее время готовые программные инструменты не справляются с обнаружением новых угроз и защитой медицинских учреждений. Так, в Великобритании злоумышленники, взломав сеть медицинской компании *Synnovis*, внедрили вредоносное ПО в ее систему[15]. Подобных фактов огромное множество как в России, так и во всем мире. При этом лица с антиобщественными взглядами пытаются:

– обойти средства защиты медицинских учреждений;

– организовать сетевые атаки с целью внедрения в медицинские организации вредоносного программного обеспечения;

– нарушить политику собственной безопасности.

Сюда же можно отнести нелегитимные действия администраторов информационных систем.

Для предотвращения крупномасштабных противоправных посягательств необходимо уделять значительное внимание собственной безопасности учреждений. Следует находить недостатки и уязвимости программного обеспечения, которые влияют на безопасность и качество обслуживания пациентов. Так, программисты уже продемонстрировали, как они могут вмешиваться в работу кардиостимуляторов и инсулиновой помпы, являющихся медицинскими изделиями, для получения дистанционного контроля над ними[16]. Получив доступ к цифровому устройству на значительном расстоянии, они могут ввести в организм пациента смертельную дозу препарата, используемого при лечении сахарного диабета. Можно предполагать, что потенциальные злоумышленники смогут взять под контроль и иное медицинское оборудование, включая медицинских роботов для проведения удаленной хирургической помощи. Во время телехирургической операции доктор удаленно управляет медицинским роботом с помощью специализированного программного и аппаратного обеспечения. Например, уязвимость была обнаружена в устройствах компании *Medtronic*[17]. Позже *Medtronic* была вынуждена привлечь сторонних специалистов для оценки безопасности своих продуктов.

В свою очередь, к правовым проблемам цифровизации отрасли здравоохранения следует отнести:

– отсутствие легального понятийно-категориального аппарата в условиях цифровизации системы здравоохранения (не выработаны определения понятиям «цифровизация», «цифровые технологии в системе здравоохранения», «цифровизация здравоохранения», «цифровое здравоохранение», «телемедицина» и т. д.);

– отсутствие в действующих стандартах оказания медицинской помощи и клинических рекомендациях Минздрава России возможности использования технологий искусственного интеллекта в целях реализации задач, возложенных на цифровое здравоохранение;

---

[12] Хакеры взялись за медицину. (2024, 29 июля). Comnews. https://www.comnews.ru/content/234514/2024-07-29/2024-w31/1008/khakery-vzyalis-za-medicinu

[13] Выжать любой ценой: медицинская отрасль лидирует по утечкам данных. (2020, 27 февраля). iz.ru https://iz.ru/975644/olga-kolentcova-anna-urmantceva/vyzhat-liuboi-tcenoi-meditcinskaia-otrasl-lidiruet-po-utechkam-dannykh

[14] Новые угрозы информационной безопасности здравоохранения (2020, 24 декабря). Touro University Illinois. https://illinois.touro.edu/news/emerging-threats-in-healthcare-information-security.php

[15] Последствия кибератак на медицинские учреждения. (2024, 20 августа). Infowatch. https://www.infowatch.ru/analytics/daydzhesty-i-obzory/posledstviya-kiberatak-na-meditsinskiye-uchrezhdeniya

[16] Хакер, нашедший дыру в кардиостимуляторах, умер при таинственных обстоятельствах. (2013, 29 июля). Cnews. https://www.cnews.ru/news/top/hakernashedshij_dyru_v_kardiostimulyatorah

[17] Там же.

– проблемы определения правового режима к сквозным медицинским технологиям и результатам их достижений (к примеру, необходим выбор оптимальной модели правового регулирования биопринтных технологий в Российской Федерации[18]);

– вопросы привлечения субъектов к юридической ответственности за действия (бездействия) при разработке (создании) и использовании (применении) медицинских изделий, разработанных на основе цифровых технологий (к примеру, медицинских роботов) (Шутова, 2024) и иные.

Учитывая дальнейшие процессы цифровизации системы здравоохранения и то, что это одно из направлений национальной безопасности Российской Федерации, необходимо обеспечить, чтобы меры цифровой безопасности были соизмеримы с имеющимися рисками.

Юридико-терминологический анализ понятия «цифровая безопасность системы здравоохранения»

Безопасность – это ключевое и комплексное понятие (Гончаров, 2009), имеющее, помимо доктринального понимания, и легальное толкование. В нормативных правовых актах Российской Федерации под термином «безопасность» понимается состояние защищенности жизненно важных интересов личности, общества и государства[19], национальных интересов[20], участников дорожного движения[21] от каких-либо угроз. В представленном исследовании мы придерживаемся уже сложившейся в национальной правовой системе России позиции относительно определения понятия «безопасность».

В свете форсированной цифровизации отрасли здравоохранения, активного внедрения цифровых технологий в различные процессы оказания медицинской помощи вопросам цифровой безопасности системы здравоохранения должно уделяться первостепенное значение. Кроме того, после совершения различных криминальных посягательств на цифровую безопасность медицинских учреждений пациенты должны продолжать получать медицинскую помощь, от которой может зависеть их жизнь и здоровье, в том числе оперироваться. В связи с этим особое место должно отдаваться охране цифровой инфраструктуры системы здравоохранения, которая нуждается в цифровой безопасности для защиты конфиденциальности, безопасности и жизни пациентов.

За последнее время злоумышленники атаковали сектор здравоохранения и использовали программы-вымогатели для предотвращения доступа к критически важным системам, в том числе электронным системам клиник и их данным, что может привести к причинению вреда жизни и здоровью пациентов. По результатам исследования, проведенного *Positive Technologies*, в 2023 г. во всем мире было зафиксировано рекордное количество атак с использованием программ шифрования цифровых данных учреждений системы здравоохранения в целях последующего вымогательства. Больше всего от таких действий пострадали медицинские организации: каждое пятое преступное посягательство на учреждения отрасли было проведено с использованием вымогательского программного обеспечения[22]. Поясним вышесказанное только некоторыми примерами из мировой практики:

1) в 2022 г. больница *Centre Hospitalier Sud Francilien*, расположенная в 28 км от центра Парижа, подверглась атаке, в результате которой клиника была вынуждена направить пациентов в другие медучреждения, а также отложить приемы больных и операции. Злоумышленники потребовали у руководства учреждения выкуп в размере 10 млн долларов в обмен на ключ дешифрования[23];

---

[18] Более подробно можно ознакомиться в монографии: Шутова, А. А. (2022). Регулирование и охрана отношений в сфере биопринтных технологий. Москва: Проспект. EDN: RQFNTB

[19] О безопасности. № 2446-I от 05.03.1992. (1992). Российская газета, 103.

[20] Указ Президента Российской Федерации № 400 от 02.07.2021. (2021). Собрание законодательства Российской Федерации, 27 (ч. II), ст. 5351.

[21] О безопасности дорожного движения. № 196-ФЗ от 10.12.1995. (1995). Собрание законодательства Российской Федерации, 50, ст. 4873.

[22] Стало известно, сколько заработали хакеры на вымогательстве в 2023 году. (2024, 25 апреля). РИА Новости. https://ria.ru/20240425/khakery-1942179115.html

[23] Французская больница срочно вывозит пациентов в другие госпитали из-за атаки программы-вымогателя. (2022, 24 августа). Cisoclub. https://cisoclub.ru/franczuzskaya-bolnicza-srochno-vyvozit-paczientov-v-drugie-gospitali-iz-za-ataki-programmy-vymogatelya/

2) в 2023 г. российская лабораторная служба «Хеликс» подверглась атаке, в результате чего была частично приостановлена работа лабораторных комплексов и наблюдались задержки в выдаче результатов. Злоумышленники попытались внедрить вредоносное программное обеспечение, которое зашифровывает файлы и блокирует работу систем. После чего потребовали денежный выкуп за программное обеспечение, способное расшифровать поврежденные данные[24];

3) с января 2022 г. по июнь 2024 г. в Италии произошло 26 случаев использования программ-вымогателей в здравоохранении, при этом она стала третьей из числа наиболее пострадавших после сфер производства и розничной торговли[25].

В результате подобных криминальных посягательств на цифровую безопасность учреждений системы здравоохранения больницам, оказывающим медицинскую помощь населению, и их пациентам, был причинен следующий вред:

1) в Германии, Великобритании и США больницы были вынуждены отменять и откладывать прием больных, сдачу анализов и переливание крови, не могли перевозить пациентов в другие лечебные учреждения[26];

2) в Великобритании в больницах не смогли определять группу крови, в результате чего пациентам переливали первую группу крови[27];

3) в Коннектикуте нападения на больницу *Manchester Memorial* привели к сбоям в работе на шесть недель, прежде чем восстановилось предоставление услуг в прежних объемах[28];

4) в результате атаки на медицинский центр «Сюд-Франсильен» в Корбей-Эссоне (недалеко от Парижа) злоумышленники опубликовали персональные данные пациентов и сведения из их медицинских карт[29];

5) была отключена система обработки платежей, которой управляла компания *Change*, принадлежащая *UnitedHealthcare*, являющейся крупной компанией здравоохранения в США. *Change* функционировала как посредник между страховщиками, поставщиками, больницами и аптеками. Больницы и другие медицинские учреждения не смогли обрабатывать счета и получать платежи, необходимые им для работы. Врачи и пациенты не смогли получить одобрение страховой выплаты на некоторые процедуры, аптеки также были затронуты[30].

Однако последствия подобных противоправных посягательств могут создать угрозу оказания медицинской помощи другим нуждающимся пациентам[31], а также невозможность проводить вовремя операции. Следовательно, последствия совершения уголовно наказуемых деяний, посягающих на цифровую безопасность системы здравоохранения, могут быть значительно серьезнее в связи с тем, что предоставление медицинских услуг зависит от применяемых цифровых решений.

---

[24] «Хеликс» предупредила о задержке выдачи результатов анализов из-за хакерской атаки. (2023, 17 июля). ТАСС. https://tass.ru/ekonomika/18295025

[25] Здравоохранение: информационная кампания по кибербезопасности начинается в регионе Лацио. (2024, 24 сентября). Агентство Нова. Ежедневное информационное агентство. https://www.agenzianova.com/ru/news/Sanita

[26] Больницы Великобритании столкнулись с беспрецедентной нехваткой крови после кибератаки. (2024, 26 июня). Азербайджанское государственное информационное агентство. https://azertag.az/ru/xeber/bolnicy_velikobritanii_stolknulis_s_besprecedentnoi_nehvatkoi_krovi_posle_kiberataki-3113306; Не успели спасти: пациентка умерла из-за хакерской атаки. (2020, 18 сентября). gazeta.ru. https://www.gazeta.ru/tech/2020/09/18/13255255/ransomware_death.shtml; Лондонские больницы сообщили о масштабном ЧП из-за кибератаки. (2024, 4 июня). Коммерсантъ. https://www.kommersant.ru/doc/6746095; Работа больницы в американском штате Айдахо была нарушена в результате кибератаки (2023, 1 июня). Interfax. https://www.interfax.ru/world/904217

[27] Больницы Великобритании столкнулись с беспрецедентной нехваткой крови после кибератаки. (2024, 26 июня). Азербайджанское государственное информационное агентство. https://azertag.az/ru/xeber/bolnicy_velikobritanii_stolknulis_s_besprecedentnoi_nehvatkoi_krovi_posle_kiberataki-3113306

[28] Последствия кибератак на медицинские учреждения. (2024, 20 августа). Infowatch. https://www.infowatch.ru/analytics/daydzhesty-i-obzory/posledstviya-kiberatak-na-meditsinskiye-uchrezhdeniya

[29] Больница во французском Ренне подверглась кибератаке, сообщили СМИ. (2023, 22 июня). РИА Новости. https://ria.ru/20230622/kiberataka-1879872152.html

[30] Российские больницы под огнем. Число кибертак на медучреждения выросло на треть. (2024, 26 июля). Cnews. https://www.cnews.ru/news/top/2024-07-26_kibertaki_na_meditsinskie

[31] Могут быть и иные угрозы для пациентов: кредитные организации, узнав диагноз, анамнез и описание состояния больного человека через покупку базы данных в DarkNet пациентов, могут отказать человеку в выдаче кредита; данные о страховании, страховых полисах и выплатах могут использоваться для мошенничества.

Далее укажем то, что с развитием цифровых технологий и постепенной эволюцией от информационного общества к цифровому вслед за информационной безопасностью появился новый термин – «цифровая безопасность».

В правовой доктрине понятие «цифровая безопасность» является не новым и используется в трудах: В. Ф. Джафарли (2019), С. Я. Лебедева (2019), Н. А. Крайновой (2019), И. Р. Бегишева (2021), Г. З. Мансурова[32], что также свидетельствует о его устойчивости и научной обоснованности. Одним из первых в юридических науках стал использовать термин «цифровая безопасность» В. Ф. Джафарли.

С точки зрения лексического понимания значение слова «цифровой» сильно изменилось: раньше оно было связано с «цифрой, числом», сейчас оно закрепляется за работой с информацией и массивами данных посредством цифр, связанный с двоичной компьютерной системой» (Бегишев, 2021).

При этом в российском законодательстве отсутствуют сегодня дефиниции «цифровая информация», «цифровые технологии», «цифровая инфраструктура», «цифровая безопасность», вместо них используются применяемые в законе термины «преступления в сфере компьютерной информации», «компьютерная информация», «информационная безопасность», «кибербезопасность».

Рассмотрим соотношение между собой информационной, кибер- и цифровой безопасности. В подпункте «в» пункта 2 Доктрины информационной безопасности Российской Федерации[33] содержится определение понятия «информационная безопасность Российской Федерации», в котором ключевым является указание на внутренние и внешние информационные угрозы. В определении также важнейшее значение приобретает употребляемое понятие «информационная угроза», которая создает опасность нанесения ущерба интересам в информационной сфере. Однако «информационная сфера» представляет собой определенную совокупность информации, информационных технологий, сайтов в сети Интернет, субъектов, занимающихся обработкой информации и других элементов. Следовательно, исходя из вышеназванного Указа Президента Российской Федерации, информационная безопасность связана с обеспечением безопасности любых данных, представленных в любой форме, в том числе и в документарной.

Далее хотелось бы уточнить то, что между информационной безопасностью и кибербезопасностью также имеются отличия. Информационная безопасность направлена на защиту информации, а кибербезопасность, представляя собой разновидность информационной технологии (Козлова, Довгаль, 2021), защищает инфраструктуру, все системы, сети и информацию в цифровой форме – данные.

Далее рассмотрим соотношение цифровой и информационной безопасности. Учитывая то, что основу цифровой безопасности составляют цифровая информация и все процессы, происходящие с ней, то в ее правовую природу закладываются именно цифровые технологии. В свою очередь, в основе любой цифровой технологии присутствует информационная составляющая. Эволюция информационных технологий привела к смене традиционных парадигм и пониманию того, что в любой цифровой технологии есть информационная составляющая, но при этом не всегда любая информационная технология является цифровой[34]. Поэтому можно сделать вывод о том, что цифровая безопасность является частью информационной и их можно рассматривать как часть и целое.

Развитие цифровых технологий, а вслед за ними систем обеспечения защиты информации определило высокую частоту использования термина «цифровая безопасность». Именно поэтому в целях исследования важным является определение цифровой безопасности системы здравоохранения и элементов, раскрывающих ее содержание.

Несмотря на использование термина «цифровая безопасность» в правовой доктрине, среди авторов, раскрывающих его содержание, имеется лишь незначительное количество исследований по этому поводу. В уголовно-правовой доктрине проводятся исследования, посвященные изучению феномена цифровой безопасности и ее элементов. Так, И. Р. Бегишев обосновывает концепцию «цифровой безопасности» через

---

[32] Мансуров, Г. З. (2022). Право цифровой безопасности: учебник. Москва: Директ-Медиа.

[33] Указ Президента Российской Федерации № 646 от 05.12.2016. (2016). Собрание законодательства Российской Федерации, 50, ст. 7074.

[34] Под цифровыми технологиями понимается разновидность технологий, в которых информация представляется в универсальном цифровом виде (числовой форме), что позволяет создавать, хранить и распространять данные. При этом цифровая информация представлена в виде битов, имеющих значение «0» и «1», что позволяет ее передавать и иным образом обрабатывать с помощью цифровых устройств, в отличие от аналоговых.

совокупность таких элементов, как безопасность цифровой информации, цифровой инфраструктуры и цифровых технологий (Бегишев, 2021).

Поддерживая мнения авторов о том, что цифровое общество трансформировалось из информационного (Жукова, Крюков, 2022), полагаем возможным рассмотреть элементы, образующие «информационную безопасность Российской Федерации», выделяемые в законодательстве. Так, в Доктрине информационной безопасности Российской Федерации указывается, что информационную сферу образуют информация, информационная инфраструктура, информационные технологии и субъекты, которые являются своеобразными элементами информационной безопасности и составляют ее основу[35].

Кроме того, представляется, что элементами цифровой безопасности системы здравоохранения, а следовательно, наполняющими ее содержание, являются своеобразные предметы преступного посягательства, в связи и по поводу которых совершаются преступления. Противоправные посягательства в системе цифрового здравоохранения в России возникают по поводу следующих предметов:

1) **цифровой информации**, так как в настоящее время в здравоохранении собираются огромные объемы данных – не только описательная информация (имя, профессия, физическое и психическое состояние, генетический профиль), но также данные, полученные с помощью датчиков окружающей среды, изображений (полученных с помощью эндоскопии, радиологических методов и т. д.) (Oliva et al., 2022). Злоумышленники заинтересованы в получении хранящихся в цифровой форме персональных данных пациентов. Так, в *DarkNet* можно легко получить доступ к более чем 1 млрд медицинских записей пациентов, и ежедневно в базу добавляются миллионы дополнительных записей (Seh et al., 2020). Незаконный сбор сведений, представляющих персональные данные пациентов, образующих институт медицинской тайны, растет, поскольку эти записи стоят дороже из-за высокой ценности подобных сведений (Offner et al., 2020).

Особая ценность цифровой информации, обращающейся в учреждениях системы здравоохранения, вызывает огромный интерес у правонарушителей, стремящихся незаконным образом получить ее и затем злоупотребить ею. Грачева с соавторами указывает, что «в зарубежных странах имеются случаи, когда для искажения работы диагностического алгоритма врачи меняли пиксели в снимке магнитно-резонансной томографии для увеличения сумм страховых выплат. В результате медицинское изделие, разработанное на основе цифровых технологий, определяло признаки болезни, которой на самом деле не было» (Грачева и др., 2020. С. 150).

Данные о здоровье и генетические данные являются наиболее важной личной информацией; они могут быть использованы для совершения преступлений. Наиболее распространенной угрозой могут стать искажение данных о здоровье пациентов и доступ к конфиденциальным сведениям об их физическом состоянии, что способно спровоцировать:

– требование передачи денежных средств, сопряженное с угрозой уничтожения или разглашения медицинских данных (о заболевании пациента, к примеру ВИЧ);

– доведение лица до самоубийства или до покушения на самоубийство путем манипулирования сведениями, которые стали известны о пациенте (серьезное заболевание, вызванное половым путем);

– склонение к совершению преступления под угрозой распространения ставших известными сведений о пациенте;

– склонение психически нездоровых пациентов к переводу денежных средств или продажи недвижимого имущества по цене ниже рыночной и др. (Грачева и др., 2020).

В результате нарушения режима неприкосновенности персональных данных и иной врачебной тайны о пациенте может наступить ряд негативных последствий:

– назначение неверной дозировки лекарственных средств и гибель пациента;

– неверный выбор метода лечения в результате подлога данных об анамнезе и выборе метода лечения пациента, что может стать причиной смерти или причинения вреда его здоровью;

– заключение эксперта о невменяемости лица, в результате изучения которого суд может признать человека невменяемым и наоборот (человек может быть растерян, что будет изучено судом как повод в признании его невменяемым);

---

[35] Указ Президента Российской Федерации № 646 от 05.12.2016. (2016). Собрание законодательства Российской Федерации, 50, ст. 7074.

– получение различных мер социальной поддержки, например, если в результате модификации данных человеку будет установлен диагноз «бронхиальная астма» или назначена инвалидность, определен инсульт, позволяющие получать лекарственные средства на льготных основаниях и затем перепродавать дороже.

Рассмотрим несколько примеров, наглядным образом иллюстрирующих то, что цифровая информация, обращающаяся в учреждениях системы здравоохранения, подвержена многочисленным противоправным посягательствам:

– в 2023 г. одна из крупнейших больниц штата Флорида – *Tampa General* – заявила, что злоумышленники похитили конфиденциальные данные более чем 1,2 млн пациентов во время атаки на учреждение[36];

– подвержен массовой атаке медицинский центр «Сюд-Франсильен» (*CHSF*) в Корбей-Эссоне (рядом с Парижем), в результате которого злоумышленники требовали передать им денежные средства в размере 10 млн долларов, не получив которые распространили персональные данные пациентов и сведения из их медицинских карт[37];

– в 2023 г. противоправным посягательствам подверглись сервисы службы скорой помощи в департаменте Ланд (Франция), в результате чего были утеряны данные всех пациентов[38];

– в 2021 г. в результате взлома крупнейшей южнокорейской больницы, университетского госпиталя Сеульского национального университета (*SNUH*) похищены конфиденциальные медицинские данные и личная информация 831 тысячи человек, большинство из которых были пациентами госпиталя. Еще 17 тысяч пострадавших – нынешние и бывшие сотрудники университета[39].

Криминальную угрозу безопасности информации, обращающейся в учреждениях системы здравоохранения, представляют действия, направленные на их незаконное собирание, распространение, блокирование и модификацию;

2) **использующихся медицинских изделий и иных устройств**, созданных на основе цифровых технологий, которые собирают и обрабатывают цифровые данные. В силу наличия программной части у медицинского изделия, созданного и работающего на основе цифровых технологий, оно, даже выраженное в материальной форме, не имеет (чаще всего) интереса для злоумышленника в качестве предмета внешнего (окружающего) мира; для них интерес представляет именно его программная составляющая, позволяющая реализовать функционал изделия в преступных целях или использовать, к примеру, возможности медицинского робота. Не стоит забывать и о возможных криминальных рисках, связанных с противоправными действиями в отношении законного оборота биопринтера, в том числе хищением биопринтера, биочернил, незаконной торговлей биопринтерами, биочернилами;

3) **посягательств на объекты критической информационной инфраструктуры**, причиняющих ущерб как гражданам, так и обществу, и государству. В жизни государства и общества огромную роль занимают объекты информационной инфраструктуры, обеспечивающие наступательное развитие цифровизации (Дремлюга и др., 2019).

Значение критической информационной инфраструктуры и противоправные посягательства на нее проиллюстрируем следующими примерами:

а) в 2020 г. в Германии в одной из больниц вследствие хакерской атаки была поражена вся информационная инфраструктура больницы, в результате чего медики не смогли оказать помощь и пациент погиб, было возбуждено дело за непредумышленное убийство[40];

---

[36] Флоридская больница допустила утечку данных пациентов во время кибератаки 2 месяца назад. (2023, 25 июля). InformationSecurity. https://www.itsec.ru/news/floridskaya-bolniza-dopustila-utechku-dannih-pazientov-vo-vremia-kiberataki-2-mesiaza-nazad.

[37] Больница во французском Ренне подверглась кибератаке, сообщили СМИ. (2023, 22 июня). РИА Новости. https://ria.ru/20230622/kiberataka-1879872152.html

[38] Там же.

[39] Северокорейские хакеры украли данные более 800 тысяч пациентов сеульской больницы. (2023, 11 мая). InformationSecurity. https://www.itsec.ru/news/severkoreyskiye-hakeri-ukrali-danniye-bolee-800-tisiach-pazientov-seulskoy-bolnizi.

[40] В Дюссельдорфе пациентка умерла после хакерской атаки на клинику. (2020, 17 сентября). ТАСС. https://tass.ru/obschestvo/9482283.

б) в 2022 г. ряд медицинских организаций Хабаровского края (включая краевую психиатрическую больницу имени профессора Галанта) попали под серьезные *DDoS*-атаки, пострадала работоспособность медицинских информационных систем этих организаций[41];

в) в 2022 г. в Нижнем Новгороде осуществлена фиктивная вакцинация от новой коронавирусной инфекции медицинской сестрой, которая внесла в систему несоответствующие действительности сведения. В отношении нее было возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 4 ст. 274^1 УК РФ[42].

Следовательно, полагаем возможным к основным элементам цифровой безопасности системы здравоохранения относить следующую триаду компонентов:

– безопасность цифровой информации, образующейся в учреждениях системы здравоохранения;

– безопасность цифровой инфраструктуры учреждений системы здравоохранения;

– безопасность цифровых технологий, используемых (применяемых) в системе здравоохранения.

Таким образом, цифровая безопасность системы здравоохранения подразумевает под собой состояние защищенности цифровой информации, цифровой инфраструктуры и цифровых технологий в системе здравоохранения от внутренних и внешних цифровых угроз.

При этом под цифровой угрозой понимается совокупность условий и факторов, создающих опасность нанесения ущерба личности, обществу и государству в цифровой сфере и направленных на нарушение безопасности цифровой информации, цифровой инфраструктуры и цифровых технологий.

Полагаем, что сформулированный нами понятийно-категориальный аппарат в целом дополнит язык уголовно-правовой науки и позволит выработать конкретное направление по совершенствованию действующего законодательства.

Ключевые криминальные риски цифровизации здравоохранения

Стоит поддержать мнение Ю. Рягина, считающего, что безрискованных видов деятельности просто не существует[43]. Сфера здравоохранения, а в особенности экспериментальная медицина, является особенно рискованным видом деятельности. Именно поэтому термин «риск» употребляется в Федеральном законе от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»[44] **16 раз**. Учитывая изначально рискованный характер медицинской деятельности, представляется, что факторы риска должны быть учтены при рассмотрении вопросов правового регулирования, а также подробно регламентированы вопросы ответственности.

Учитывая, что предметами преступных посягательств против цифровой безопасности системы здравоохранения выступают цифровая информация, критическая информационная инфраструктура Российской Федерации и цифровые технологии (кроме того, последние могут выступать средствами совершения преступлений), то выделим следующие криминальные риски цифровизации здравоохранения:

– криминальные риски, возникающие в связи с обращением цифровой информации в системе здравоохранения;

– криминальные риски, свойственные медицинским изделиям, разработанным на основе цифровых технологий;

– криминальные риски критической информационной инфраструктуры Российской Федерации.

Полагаем, что наиболее сложную систему криминальных рисков представляют собой риски, свойственные медицинским изделиям, разработанным на основе цифровых технологий, в связи с огромным количеством применяемых инновационных решений и множеством субъектов, вовлекаемых в их оборот, жизненного

---

[41] Хакеры атаковали больницы в Хабаровском крае. (2022, 30 марта). D-Russia. https://d-russia.ru/hakery-atakovali-bolnicy-v-habarovskom-krae.html

[42] СК расследует дела о фиктивной вакцинации от ковида. (2022, 30 января). RG.ru. https://rg.ru/2022/01/30/reg-dfo/sk-rassleduet-dela-o-fiktivnoj-vakcinacii-ot-kovida.html

[43] Рягин, Ю. (2012). Рискология: учебник для вузов: в 2 ч. ч. 1 М.: Юрайт. 255 с.

[44] Федеральный закон Российской Федерации № 323-ФЗ от 21.11.2011. (2011). Собрание законодательства Российской Федерации, 48, ст. 6724.

цикла медицинского изделия. В связи с этим система криминальных рисков той или иной цифровой здравоохранительной технологии будет уникальной, отличающейся от другой. Рассмотрим криминальные риски некоторых цифровых технологий, применяемых в здравоохранении, – технологии медицинской робототехники, технологии искусственного интеллекта.

Несомненно, для оценки уровня риска применения медицинских изделий, разработанных на основе цифровых технологий, в том числе «искусственного интеллекта, предполагается использование двух основных критериев: степень зависимости пользователей от принимаемых системой решений и степень ее опасности для жизни и здоровья граждан и нарушения их основных прав» (Эрахтина, 2023).

Ранее мы исследовали систему криминальных рисков, свойственных медицинским изделиям, разработанным на основе цифровых технологий (Шутова, 2024):

– *криминальные риски, действующие на медицинского робота извне* (риски, исходящие от злоумышленников в результате неправомерного доступа к медицинскому роботу; риски, исходящие от медицинского персонала в процессе эксплуатации медицинского робота; риски, исходящие от персонала, занимающегося ремонтом, сервисным обслуживанием медицинского робота (его основных частей (модулей)); риски, исходящие от пациента;

– *криминальные риски, свойственные медицинскому роботу* (незаметные внутренние нарушения; отказ от обслуживания; неправильные результаты измерений или показателей до полного отказа и нанесения вреда окружающей среде, вреда жизни или здоровью граждан);

– *криминальные риски, исходящие от медицинского робота* (связаны с конструкцией медицинского робота (острый скальпель, острый кончик консоли); окружением (электричество, рентгеновские лучи и т. д.); воздействием (электричество, рентгеновские, лазерные лучи, холод и т. д.).

Далее представим авторскую концепцию классификации криминальных рисков, связанных с созданием и применением медицинских изделий на основе технологий искусственного интеллекта, по этапам жизненного цикла медицинского изделия[45]:

I этап. Криминальные риски создания (разработки) медицинского изделия на основе технологий искусственного интеллекта. Значительным риском для искусственного интеллекта является отсутствие прозрачности в отношении этапов: проектирования, разработки, оценки и внедрения технологий искусственного интеллекта в систему здравоохранения.

II этап. Криминальные риски применения в медицинской практике медицинских изделий на основе технологий искусственного интеллекта (имеются риски в отношении конфиденциальности и безопасности данных пациентов, а также риски совершения неправомерного воздействия на медицинские изделия, разработанные на основе технологий искусственного интеллекта). По субъекту данные риски можно поделить на риски, исходящие от медицинского персонала в процессе применения медицинских изделий, оснащенных технологиями искусственного интеллекта; риски, исходящие от персонала, занимающегося ремонтом, сервисным обслуживанием, утилизацией медицинских изделий, оснащенных технологиями искусственного интеллекта; риски, исходящие от злоумышленников в результате неправомерного доступа к медицинскому изделию, оснащенному технологией искусственного интеллекта; риски, исходящие от пациента.

III этап. Криминальные риски утилизации медицинских изделий на основе технологий искусственного интеллекта (неверная утилизация медицинских изделий на основе технологий искусственного интеллекта создает риск незаконного распространения персональных данных и иной служебной информации, обращающейся в изделии).

Очевидно, что перечисленные криминальные риски создают базис потребности на уголовно-правовую охрану цифровой безопасности в системе здравоохранения.

[45] Более подробно с криминальными рисками, связанными с созданием и применением медицинских изделий на основе технологий искусственного интеллекта, по этапам жизненного цикла медицинского изделия можно ознакомиться в работе (Шутова, Бегишев, 2023).

Запрос на уголовно-правовую охрану цифровой безопасности системы здравоохранения

Запрос на уголовно-правовую охрану цифровой безопасности системы здравоохранения обусловлен целым комплексом причин:

– форсированной цифровизацией всего здравоохранения и в связи с этим не менее ускоренными темпами развития цифровых технологий (медицинской робототехники, искусственного интеллекта, биопринтинга и других), с использованием которых или в отношении которых могут быть совершены уголовно наказуемые деяния. Возможности цифровых технологий облегчают процесс совершения противоправного деяния и позволяют совершать подобные деяния в отношении множества потерпевших (Русскевич, 2022);

– рисками взлома или несанкционированного доступа к медицинским изделиям, созданным на основе цифровых технологий. Имеется множество сведений о том, что злоумышленники, получив доступ к медицинскому устройству, не позволяли медицинским организациям предоставлять необходимое жизненно важное лечение пациентам. Так, в 2017 г. в США зафиксировано первое противоправное посягательство на облачный сервис онкологической больницы путем использования вируса-вымогателя *WannaCry*, в результате чего вышло из строя медицинское оборудование (радиологические и иные приборы, используемые в целях оказания медицинской помощи, и пациентам с онкологией пришлось перенести лучевую терапию[46]. Ситуацию ухудшает тот факт, что цифровые устройства, используемые для обмена данными пациентов, бывают не зашифрованы и уязвимы для преступников. По мнению исследователей, системы здравоохранения подключены к открытой среде (например, информационно-телекоммуникационной сети Интернет) через уязвимые протоколы связи (Магомедов, 2020), что также делает сферу здравоохранения уязвимой перед цифровыми угрозами;

– новым сквозным характером цифровых технологий, применение которых в системе здравоохранения может стать причиной причинения вреда жизни и здоровью пациентов и наступлению иных негативных процессов;

– отсутствием у некоторых учреждений системы здравоохранения технологических возможностей, позволяющих повысить цифровую безопасность медицинских изделий (Карпов и др., 2017). Приложения демонстрируют значительные недостатки в безопасности, включая использование слабых методов аутентификации и отсутствие соответствующих механизмов безопасности от цифровых угроз, которые создают риск утечки конфиденциальных данных о пациентах. Медицинские изделия, разработанные на основе цифровых технологий, обрабатывают значительные массивы данных, поэтому неправомерный доступ к ним может поставить под угрозу безопасность самого пациента, когда, к примеру, будет осуществлен захват управления изделием и его данных. Нападения такого типа могут поставить под угрозу их жизнь из-за изменения в них медицинских записей, делающих дальнейшие медицинские назначения врачей ошибочными. Именно поэтому стоит значительное внимание уделять обучению медицинских работников и пациентов безопасному обращению с системой искусственного интеллекта, чтобы избежать утечки данных и некорректного использования устройств (Галлезе-Нобиле, 2023);

– загруженностью медицинских работников на работе, что не оставляет им возможности пройти дополнительное обучение или повысить свою квалификацию по вопросам цифровой безопасности системы здравоохранения и способам ее обеспечения. Для того чтобы система здравоохранения могла воспользоваться преимуществами цифровых инструментов, каждый, кто работает в этой области, должен понимать, каким образом цифровые инструменты могут ухудшить здоровье и усугубить проблемы общественного здравоохранения, независимо от того, является ли этот вклад причинным, способствующим или благоприятным;

– повышенной общественной опасностью противоправных посягательств в сфере цифрового здравоохранения. Негативные последствия от преступлений в цифровой среде могут быть самыми различными и влиять на безопасность пациентов и оказание им медицинской помощи. Например, при посягательстве на медицинскую организацию злоумышленники могут получить доступ к конфиденциальной информации о пациентах, включая персональные данные, истории болезни и даже финансовую информацию. Противоправные посягательства с применением программ-вымогателей, блокирующих доступ к критически важным системам медицинской информации, вызывают перебои в работе, приводя к отмене амбулаторных приемов и плановых хирургических

[46] Атаки на здоровье: какие кибервызовы стоят перед современной медициной. (2022, 24 ноября). РБК. https://trends.rbc.ru/trends/industry/637f2a909a794747ebe66926?from=copy

операций. Так, в ходе серьезных атак отделениям неотложной помощи приходится отказываться от приема пациентов, доставляемых скорой помощью, а онкологическим центрам – откладывать лечение своих пациентов[47];

– противоправными посягательствами на цифровую безопасность системы здравоохранения, от которых могут пострадать самые разнообразные общественные отношения, охраняемые уголовным законом, в том числе интересы собственности, отношения, охраняющие жизнь и здоровье граждан, и т. д. Помимо посягательств на жизнь и здоровье граждан (пациентов и медицинских работников), противоправный вред причиняется системе здравоохранения, в целом подрывается ее авторитет, формируется негативное общественное отношение к отрасли среди населения;

– здравоохранение является привлекательной целью для злоумышленников в связи с тем, что медицинские данные, в том числе персональные данные пациентов, являются достаточно ценными в силу их конфиденциальности. Незаконным образом собранные медицинские записи могут быть использованы в целях совершения преступлений, к примеру, шантажа или вымогательства.

Итак, здравоохранение, в том числе цифровое, затрагивает самое ценное, что есть у человека, – его жизнь и здоровье, что обуславливает потребность в его уголовно-правовой охране и обеспечении его безопасности. Преступления против цифровой безопасности системы здравоохранения ставят под угрозу всю национальную безопасность государства, обеспечивающего достойный уровень жизни граждан. При этом юридическая регламентация общественных отношений, возникающих в сфере цифрового здравоохранения, создает естественное препятствие для реализации преступных намерений лиц, посягающих на цифровую безопасность. Упорядочивание отношений позволяет выявить круг существующих интересов, испытывающих потребность в уголовно-правовой охране.

Заключение

Здравоохранение является одной из самых важных сфер общественной жизни, от качества которой зависит продолжительность жизни и здоровья граждан в целом. В связи с форсированной цифровизацией отрасли здравоохранения, переходом ее на новый инновационный режим злоумышленники также активизировали свою преступную деятельность в данном направлении. Поэтому вопросам обеспечения цифровой безопасности системы здравоохранения должно уделяться больше внимания. Исходя из этого в исследовании была поставлена цель, которая последовательно решалась путем постановки задач.

Были определены тенденции в сфере цифрового здравоохранения, выявлены элементы цифровой безопасности системы здравоохранения, определен объем значения представленного понятия, проведен юридико-терминологический анализ понятия «цифровая безопасность системы здравоохранения», выявлен запрос на уголовно-правовую охрану цифрового здравоохранения, в результате чего на основе выявления ключевых криминальных рисков сформирована теоретическая концепция уголовно-правовой охраны цифрового здравоохранения.

Список литературы

Бахтеев, Д. В. (2023). Этико-правовые модели взаимодействия общества с технологиями искусственного интеллекта. *Журнал цифровых технологий и права*, *1*(2), 520–539. https://doi.org/10.21202/jdtl.2023.22

Бегишев, И. Р. (2021). Семантический анализ термина «цифровая безопасность». *Юрислингвистика*, *20*(31), 24–38. https://doi.org/10.14258/leglin(2021)2005

Галлезе-Нобиле, К. (2023). Правовые аспекты использования искусственного интеллекта в телемедицине. *Journal of Digital Technologies and Law*, *1*(2), 314–336. https://doi.org/10.21202/jdtl.2023.13

Гончаров, И. В. (2009). О соотношении понятий «Национальная безопасность», «Государственная безопасность», «Конституционная безопасность». *Актуальные проблемы российского права*, *1*, 116–122.

Грачева, Ю. В., Коробеев, А. И., Маликов, С. В., Чучаев, А. И. (2020). Уголовно-правовые риски в сфере цифровых технологий: проблемы и предложения. *Lex Russica*, *1*(158), 145–159. https://doi.org/10.17803/1729-5920.2020.158.1.145-159

[47] Всемирная организация здравоохранения. (2024, 6 февраля). Кибератаки на объекты критической инфраструктуры здравоохранения. https://www.who.int/ru/news-room/questions-and-answers/item/cyber-attacks-on-critical-health-infrastructure.

Джафарли, В. Ф. (2019). О созвучности тезиса «Цифровая безопасность – цифровой уголовно-правовой ресурс» теории криминологической безопасности в сфере информационных технологий. *Криминология: вчера, сегодня, завтра*, *4*(55). https://cyberleninka.ru/article/n/o-sozvuchnosti-tezisa-tsifrovoy-bezopasnosti-tsifrovoy-ugolovno-pravovoy-resurs-teorii-kriminologicheskoy-bezopasnosti-v-sfere

Дремлюга, Р. И., Зотов С. С., Павлинская В. Ю. (2019). Критическая информационная инфраструктура как предмет преступного посягательства. *Азиатско-Тихоокеанский регион: экономика, политика, право*, *2*(21), 130–139. https://doi.org/10.24866/1813-3274/2019-2/130-139

Ефремова, М. А. (2018). *Уголовно-правовая охрана информационной безопасности*. Москва: Юрлитинформ.

Жарова, А. К. (2023). Достижение алгоритмической прозрачности и управление рисками информационной безопасности при принятии решений без вмешательства человека: правовые подходы. *Journal of Digital Technologies and Law*, *1*(4), 973–993. https://doi.org/10.21202/jdtl.2023.42

Жукова, М. В., Крюков, Д. В. (2022). Современный тренд развития экономики и общества: цифровое общество как особая стадия информационного общества. *Society and Security Insights*, *5*(2), 120–139. https://doi.org/10.14258/ssi(2022)2-08

Карпов, О. Э., Субботин, С. А., Шишканов Д. В., Замятин, М. Н. (2017). Цифровое здравоохранение. Необходимость и предпосылки. *Врач и информационные технологии*, 3, 6–22.

Козлова, Н. Ш., Довгаль, В. А. (2021). Кибербезопасность и информационная безопасность: сходства и отличия. *Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки*, *3*(286), 88–97. https://doi.org/10.53598/2410-3225-2021-3-286-88-97

Крайнова, Н. А. (2019). «Международная цифровая безопасность»: миф или реальность? *Криминология: вчера, сегодня, завтра*, *4*(55), 42–46.

Лебедев, С. Я. (2019). Цифровой безопасности – цифровой уголовно-правовой ресурс. *Криминология: вчера, сегодня, завтра*, *4*(55), 17–25.

Магомедов, Ш. Г. (2020). Анализ защиты компьютерных сетей и приложений информационных процессов учреждений здравоохранения. *Cloud of Science*, *7*(3), 685–704.

Пучков, Д. В. (2022). *Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики*: автореф. … д-ра юрид. наук. Екатеринбург.

Русскевич, Е. А. (2022). *Уголовное право и «цифровая преступность»: проблемы и решения*: монография (2-е изд., перераб. и доп.). Москва: ИНФРА-М.

Ткаченко, И. Н., Чеснюкова, Л. К. (2023). Цифровые технологии в сфере здравоохранения как способ обеспечения качества человеческого капитала. *Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право*, *2*(23), 163–173. https://doi.org/10.18500/1994-2540-2023-23-2-163-173

Файн, А., Ли, С., Миллер, М. (2024). Контент-анализ мнений судей об инструментах оценки рисков с использованием искусственного интеллекта. *Russian Journal of Economics and Law*, *18*(1), 246–263. https://doi.org/10.21202/2782-2923.2024.1.246-263

Чупрова, А. Ю. (2015). *Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции*: дис. … д-ра юрид наук.

Шутова, А. А. (2023). Угрозы информационной безопасности учреждений системы здравоохранения: уголовно-правовой аспект. *Вестник Уфимского юридического института МВД России*, *3*(101), 131–137.

Шутова, А. А. (2024). *Уголовно-правовая охрана медицинской робототехники*. Москва: Проспект. https://doi.org/10.31085/9785392405183-2024-88

Шутова, А. А., Бегишев, И. Р. (2023). Проект Этического кодекса субъектов, осуществляющих деятельность по созданию, применению и утилизации медицинских изделий на основе технологий искусственного интеллекта. *Russian Journal of Economics and Law*, *17*(4), 873–881. https://doi.org/10.21202/2782-2923.2023.3.873-881

Эрахтина, О. С. (2023). Подходы к регулированию отношений в сфере разработки и использования технологий искусственного интеллекта: особенности и практическое применение. *Журнал цифровых технологий и права*, *1*(2), 421–437. https://doi.org/10.21202/jdtl.2023.17

Ядав, Н. (2023). Этика искусственного интеллекта и робототехники: ключевые проблемы и современные способы их решения. *Journal of Digital Technologies and Law*, *1*(4), 955–972. https://doi.org/10.21202/jdtl.2023.41

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University – Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Argaw, S. T., Troncoso-Pastoriza, J., Lacey, D., Florinm M., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1), 146. https://doi.org/10.1186/s12911-020-01161-7

Borges do Nascimento, I. J., Abdulazeem, H. M., Vasanthan, L. T., Martinez, E. Z., Zucoloto, M. L., Østengaard, L., Azzopardi-Muscat, N., Zapata, T., & Novillo-Ortiz, D. (2023). The global effect of digital health technologies on health workers' competencies and health workplace: an umbrella review of systematic reviews and lexical-based and sentence-based meta-analysis. *Lancet Digit Health*, *5*(8), e534-e544. https://doi.org/10.1016/s2589-7500(23)00092-4

Martínez-Caro, E., Cegarra-Navarro, J. G., & Solano-Lorente, M. (2013). Understanding patient e-loyalty toward online health care services. *Health Care Management Review*, *38*(1), 61–70. https://doi.org/10.1097/hmr.0b013e31824b1c6b

Morgan, S. (2020). *The 2020-2021 Healthcare Cybersecurity Report*. Herjavec Group.

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intelligence and National Security*, *35*(4), 556–585. https://doi.org/10.1080/02684527.2020.1752459

Oliva, A, Grassi, S., Vetrugno, G., Rossi, R., Della Morte, G., Pinchi, V., & Caputo, M. (2021). Management of Medico-Legal Risks in Digital Health Era: A Scoping Review. *Frontiers in Medicine*, 8, 821756. https://doi.org/10.3389/fmed.2021.821756

She, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, *8*(2), 133. https://doi.org/10.3390/healthcare8020133

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

References

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University – Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Argaw, S. T., Troncoso-Pastoriza, J., Lacey, D., Florinm M., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1), 146. https://doi.org/10.1186/s12911-020-01161-7

Bakhteev, D. V. (2023). Ethical-Legal Models of the Society Interactions with the Artificial Intelligence Technology. *Journal of Digital Technologies and Law*, *1*(2), 520–539. (In Russ.). https://doi.org/10.21202/jdtl.2023.22

Begishev, I. (2021). Semantic Analysis of the Term "Digital Security". *Legal Linguistics*, *20*(31), 24–38. (In Russ.). https://doi.org/10.14258/leglin(2021)2005

Borges do Nascimento, I. J., Abdulazeem, H. M., Vasanthan, L. T., Martinez, E. Z., Zucoloto, M. L., Østengaard, L., Azzopardi-Muscat, N., Zapata, T., & Novillo-Ortiz, D. (2023). The global effect of digital health technologies on health workers' competencies and health workplace: an umbrella review of systematic reviews and lexical-based and sentence-based meta-analysis. *Lancet Digit Health*, *5*(8), e534-e544. https://doi.org/10.1016/s2589-7500(23)00092-4

Chuprova, A. Yu. (2015). *Criminal-legal mechanisms of regulating relations in the sphere of electronic commerce*: Dr. Sci. (Law) thesis.

Dremlyuga, R. I., Zotov, S. S., & Pavlinskaya, V. Yu. (2019). Critical informational infrastructure as object of a criminal offence. *PACIFIC RIM: Economics, Politics, Law*, *2*(21), 130–139. (In Russ.). https://doi.org/10.24866/1813-3274/2019-2/130-139

Dzhafarli, V. F. (2019). On the consonance between the thesis "Digital criminal law resource for digital security" and the theory of criminological security in it sphere. *Kriminology: Yesturday, today, tomorrow*, *4*(55). (In Russ.). https://cyberleninka.ru/article/n/o-sozvuchnosti-tezisa-tsifrovoy-bezopasnosti-tsifrovoy-ugolovno-pravovoy-resurs-teorii-kriminologicheskoy-bezopasnosti-v-sfere

Efremova, M. A. (2018). *Criminal-legal protection of information security*. Moscow: Yurlitinform. (In Russ.).

Erahtina, O. S. (2023). Approaches to Regulating Relations in the Sphere of Developing and Using the Artificial Intelligence Technologies: Features and Practical Applicability. *Journal of Digital Technologies and Law*, *1*(2), 421–437. (In Russ.). https://doi.org/10.21202/jdtl.2023.17

Fine A., Le S., & Miller M. (2024). Content Analysis of Judges' Sentiments Toward Artificial Intelligence Risk Assessment Tools. *Russian Journal of Economics and Law*, *18*(1), 246–263. (In Russ.). https://doi.org/10.21202/2782-2923.2024.1.246-263

Fine, A., Lee, S., Miller, M. (2024). Content analysis of judges' opinions on risk assessment tools using artificial intelligence. *Russian Journal of Economics and Law, 18*(1), 246–263. https://doi.org/10.21202/2782-2923.2024.1.246-263

Gallese Nobile C. (2023). Legal Aspects of the Use Artificial Intelligence in Telemedicine. *Journal of Digital Technologies and Law*, *1*(2), 314–336. https://doi.org/10.21202/jdtl.2023.13

Goncharov, I. V. (2009). On the correlation between the notions "National security", "State security", "Constitutional security". *Actual Problems of Russian Law*, *1*, 116–122. (In Russ.).

Gracheva, Yu. V., Korobeev, A. I., Malikov, S. V., & Chuchaev, A. I. (2020). Criminal and Legal Risks in the Field of Digital Technologies: Problems and Suggestions. *Lex Russica*, *1*(158), 145–159. https://doi.org/10.17803/1729-5920.2020.158.1.145-159

Jukova, M. V., & Kryukov, D. V. (2022). Modern trend in the development of the economy and society: digital society as a special stage of the information society. *Society and Security Insights*, *5*(2), 120–139. https://doi.org/10.14258/ssi(2022)2-08

Karpov, O.E., Subbotin, S.A., Shishkanov, D.V., & Zamyatin, M.N. (2017). Digital public health. Necessity and background. *Medical Doctor and Information Technologies*, 3, 6–22. (In Russ.).

Kozlova, N. Sh., & Dovgal, V. A. (2021). Cybersecurity and information security: similarities and differences. *Bulletin of Adygea State University. Series 4: Natural, mathematical and technical sciences*, *3*(286), 88–97. https://doi.org/10.53598/2410-3225-2021-3-286-88-97

Krainova, N. A. (2019). "International digital security": myth or reality? *Kriminology: Yesturday, Today, Tomorrow*, *4*(55), 42–46. (In Russ.).

Lebedev, S. Ya. (2019). Digital criminal law resource for digital security. *Kriminology: Yesturday, Today, Tomorrow*, *4*(55), 17–25. (In Russ.).

Magomedov, S. G. (2020). Security analysis of computer networks and applications of the healthcare organizations information processes. *Cloud of Science*, *7*(3), 685–704. (In Russ.).

Martínez-Caro, E., Cegarra-Navarro, J. G., & Solano-Lorente, M. (2013). Understanding patient e-loyalty toward online health care services. *Health Care Management Review*, *38*(1), 61–70. https://doi.org/10.1097/hmr.0b013e31824b1c6b

Morgan, S. (2020). *The 2020-2021 Healthcare Cybersecurity Report*. Herjavec Group.

Mosechkin, I. N. (2023). The Concept of Crimes against Digital Data Security. *Lex Russica*, *76*(5), 49–59. (In Russ.). https://doi.org/10.17803/1729-5920.2023.198.5.049-059

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intelligence and National Security*, *35*(4), 556–585. https://doi.org/10.1080/02684527.2020.1752459

Oliva, A, Grassi, S., Vetrugno, G., Rossi, R., Della Morte, G., Pinchi, V., & Caputo, M. (2021). Management of Medico-Legal Risks in Digital Health Era: A Scoping Review. *Frontiers in Medicine*, 8, 821756. https://doi.org/10.3389/fmed.2021.821756

Puchkov, D. V. (2022). *Criminal-legal model of protecting telecommunications against criminal infringements: problems of theory and practice*: abstract of Dr. Sci. (Law) thesis. Ekaterinburg. (In Russ.).

Russkevich, E. A. (2022). *Criminal law and "digital crime": problems and solutions*: monograph (2nd ed., amended and compl.). Moscow: INFRA-M. (In Russ.).

She, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, *8*(2), 133. https://doi.org/10.3390/healthcare8020133

Shutova, A. A. (2023). Threats to the information security of healthcare institutions: criminal-legal aspect. *Bulletin of Ufa Law Institute of MIA of Russia*, *3*(101), 131–137. (In Russ.).

Shutova, A. A. (2024). *Criminal legal protection of medical robotics*. Moscow: Prospect. (In Russ.). https://doi.org/10.31085/9785392405183-2024-88

Shutova, A. A., & Begishev, I. R. (2023). Draft of an ethical code of subjects implementing activity of creating, applying and utilizing medical products based on artificial intelligence technologies. *Russian Journal of Economics and Law*, *17*(4), 873–881. https://doi.org/10.21202/2782-2923.2023.3.873-881

Tkachenko, I. N., & Chesnyukova, L. K. (2023). Digital technologies in the sphere of health care as a way to ensure the quality of human capital. *Izvestiya of Saratov University. New series. Economics. Management. Law Series*, *2*(23), 163–173. (In Russ.). https://doi.org/10.18500/1994-2540-2023-23-2-163-173

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

Yadav, N. (2023). Ethics of Artificial Intelligence and Robotics: Key Issues and Modern Ways to Solve Them. *Journal of Digital Technologies and Law*, *1*(4), 955–972. https://doi.org/10.21202/jdtl.2023.41

Zharova, A. K. (2023). Achieving Algorithmic Transparency and Managing Risks of Data Security when Making Decisions without Human Interference: Legal Approaches. *Journal of Digital Technologies and Law*, *1*(4), 973–993. https://doi.org/10.21202/jdtl.2023.42

Zhukova, M. V., Kryukov, D. V. (2022). Modern trend in the development of economy and society: digital society as a special stage of the information society. *Society and Security Insights, 5*(2), 120-139. https://doi.org/10.14258/ssi(2022)2-08

Вклад автора

Автор подтверждает, что полностью отвечает за все аспекты представленной работы.

Author's contribution

The author confirms sole responsibility for all aspects of the work.

Конфликт интересов / Conflict of Interest

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

История статьи / Article history

Дата поступления / Received 14.07.2024
Дата одобрения после рецензирования / Date of approval after reviewing 21.10.2024
Дата принятия в печать / Accepted 21.10.2024