Научная статья
УДК 616-082: 617.7
doi: 10.25276/0235-4160-2022-4S-132-137

Нормативно-правовые проблемы безопасности территориально распределенных информационных систем в офтальмологии

Д.В. Сахаров, А.И. Пешков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург

РЕФЕРАТ

Цель. Рассмотреть, содержательно охарактеризовать и проанализировать нормативно-правовую базу Российской Федерации, определяющую использование в офтальмологии информационных технологий, без которых сейчас невозможно предоставление высокотехнологической медицинской помощи. **Материал и методы.** Предметом данного исследования является законодательство РФ, посвященное как непосредственно системе здравоохранения в нашей стране, так и требованиям к обеспечению информационной безопасности. В соответствии со спецификой изучаемого предмета в данной работе применялись общенаучные методы исследования: анализ и синтез, дедукция и индукция. **Результаты.** Правовая система РФ не настолько специализирована в отношении использования информационных технологий в медицине, чтобы в офтальмологии была бы какая-то особая нормативно-правовая база, отличная от других видов медицинской деятельности. Объективной основой этой универсальности является то, что везде применяется в медицине фактически одна и та же технологическая база. **Результаты.** Наличие всех необходимых условий, определяющих принадлежность к статусу субъекта критической информационной инфраструктуры, создает достаточные основания для применения требований, связанных с регламентацией медицинской деятельности на основе Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

Ключевые слова: *медицина, информационные технологии, информационная безопасность, критическая информационная структура РФ* ■

Для цитирования: Сахаров Д.В., Пешков А.И. Нормативно-правовые проблемы безопасности территориально распределенных информационных систем в офтальмологии. Офтальмохирургия. 2022;4S: 132–137. doi: 10.25276/0235-4160-2022-4S-132-137
Автор, ответственный за переписку: Андрей Иванович Пешков, ap2000@yandex.ru

ABSTRACT

Original article

Regulatory and legal problems of security of territorially distributed information systems in ophthalmology

D.V. Sakharov, A.I. Peshkov

The Bonch-Bruevich Saint Petersburg State University of Telecommunications, Saint Petersburg, Russian Federation

Purpose. To consider, characterize and analyze the regulatory framework of the Russian Federation, which determines the use of information technologies in ophthalmology, without which it is now impossible to provide high-tech medical care. **Material and methods.** The subject of this study is the legislation of the Russian Federation devoted both directly to the health care system in our country and to the requirements for ensuring information security. In accordance with the specifics of the subject under study, general scientific research methods were necessarily used in this work: analysis and synthesis, deduction and induction. **Results.** The legal system of the Russian Federation is not so specialized in the use of information technologies in medicine that in ophthalmology there would be some special regulatory framework, different from other types of medical activities. The objective basis of this universality is that it is practically the same technological base everywhere in medicine. **Conclusion.** The presence of all the necessary conditions determining belonging to the status of a subject of critical information infrastructure creates sufficient grounds for the applying of requirements related to the regulation of medical activities based on the Federal law «On the Security of Critical Information Infrastructure of the Russian Federation».

Keywords: medicine, information technology, information security, critical information structure of the Russian Federation ■

For quoting: Sakharov D.V., Peshkov A.I. Regulatory and legal problems of security of territorially distributed information systems in ophthalmology. Fyodorov Journal of Ophthalmic Surgery. 2022;4S: 132–137. doi: 10.25276/0235-4160-2022-4S-132-137
Corresponding author: Andrei I. Peshkov, ap2000@yandex.ru

АКТУАЛЬНОСТЬ

Современная медицина в целом и офтальмология в частности не находятся вне процесса информатизации, который в настоящее время начинает охватывать все более широкие стороны их деятельности. Применение информационных технологий значительно улучшает качество, скорость, точность и эффективность предоставляемой медицинской помощи.

Организации здравоохранения сейчас повсеместно заменяют разрозненные системы ведения документооборота, осуществляемого вручную, централизованными или сетевыми территориально распределенными информационными системами, которые улучшают доступ к медицинским данным пациентов. Оцифровывание медицинской документации делает возможным автоматизированные операции с ней, которая может легко передаваться в процессе диагностики и лечения всем сторонам, участвующим в предоставлении медицинских услуг, что, в свою очередь, обеспечивает получение пациентами медицинской помощи более высокого качества при одновременном снижении затрат на администрирование этой деятельности.

ЦЕЛЬ

Рассмотреть, содержательно охарактеризовать и проанализировать нормативно-правовую базу Российской Федерации, определяющую использование в офтальмологии информационных технологий, без которых сейчас невозможно предоставление высокотехнологической медицинской помощи.

МАТЕРИАЛ И МЕТОДЫ

Предметом данного исследования является законодательство РФ, посвященное как непосредственно системе здравоохранения в нашей стране, так и требованиям к обеспечению информационной безопасности. В соответствии со спецификой изучаемого предмета в данной работе с необходимостью применялись общенаучные методы исследования: анализ и синтез, дедукция и индукция.

РЕЗУЛЬТАТЫ

При признании неоспоримых достижений в медицине, связанных с применением информационных технологий в здравоохранении, нельзя забывать, что реализуемые сейчас методы и алгоритмы искусственного интеллекта (ИИ), по терминологии Джона Серла, относятся все же к слабому, а не сильному ИИ. Как справедливо отмечает Антонио Лието, предположение о том, что когнитивные системы ИИ является частью сильного ИИ, ошибочно и проблематично, потому что «искусственные модели мозга и разума можно использовать для понимания психических явлений, не претендуя на то, чтобы быть реальными явлениями, которые они моделируют» [1]. Иначе говоря, даже сейчас диагностируют и лечат медицинские работники, а не алгоритмы ИИ. В результате этого проблемы обеспечения безопасности, возникающие в связи широким использованием информационных технологий в медицине, не сводятся только к своей технической составляющей (аппаратным и программным средствам защиты), а имеют также нормативно-правовое измерение. Именно из этого и исходит законодательство РФ, когда в статье 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определяет защиту информации как «принятие правовых, организационных и технических мер, направленных на решение трех задач:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации» [2].

Переход к централизованным и территориально распределенным информационным системам в медицине имеет своей оборотной стороной неизбежную агрегацию обрабатываемых данных, что не может не создавать угрозы в отношении их безопасности. Хорошо известно, что вероятность раскрытия информация ненадлежащим образом напрямую зависит от ее ценности и количества людей, имеющих к ней доступ: агрегирование усиливает одновременно оба этих фактора при использовании как в централизованных, так и территориально распределенных информационных системах.

До настоящего времени конфиденциальность информации, как правило, технологически обеспечивалась через ее фрагментацию и распределение по автономным компьютерам и так называемым manual systems. Устранение этого механизма обеспечения безопасности в результате создания централизованных и территориально распределенных информационных систем в медицине [3, 4] требует эффективного компенсирующего контроля, на что и направлено сейчас законодательство РФ.

Конституционно-правовая система Российской Федерации, установив принцип приоритета прав человека (статьи 2 и 18 Конституции РФ), в то же время в ч. 3 ст. 17 Конституции РФ определила, что осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц [5].

Соответственно, в ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» ин-

формация о состоянии здоровья отнесена к специальной категории персональных данных, обработка которых не допускается, за исключением не только случая, когда субъект персональных данных сам дал свое согласие в письменной форме на обработку своих персональных данных, но и по другим основаниям.

Непосредственно проблематике информационного обеспечения в сфере здравоохранения посвящена ст. 91 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», который вместе со ст. 41 Конституции РФ является базовым для системы оказания медицинской помощи в нашей стране. Согласно ч. 1 ст. 91 этого федерального закона информационное обеспечение в сфере здравоохранения осуществляется в РФ посредством создания, развития и эксплуатации следующих информационных систем:

1. Федеральные государственные информационные системы в сфере здравоохранения.

2. Информационные системы в сфере здравоохранения Федерального фонда обязательного медицинского страхования и территориальных фондов обязательного медицинского страхования.

3. Государственные информационные системы в сфере здравоохранения субъектов Российской Федерации;

4. Медицинские информационные системы медицинских организаций;

5. Информационные системы фармацевтических организаций [6].

Именно только эти пять типов информационных систем законодатель обобщенно определяет как информационные системы в сфере здравоохранения (ч. 1 ст. 91 323-ФЗ) и делегирует полномочия уполномоченному федеральному органу исполнительной власти установить требования, предъявляемые к ним (ч. 4 ст. 91 323-ФЗ). Во исполнение Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» Правительство РФ приняло постановление от 09.02.2022 № 140 «О единой государственной информационной системе в сфере здравоохранения», вступившее в силу с 1 марта 2022 г. и действующее 6 лет со дня его вступления в силу, а Министерство здравоохранения РФ издало приказ от 24 декабря 2018 г. № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций», который вступил в силу с 1 января 2020 г.

В данных нормативно-правовых актах, имеющих подзаконный характер, дается достаточно детальная характеристика информационных систем в сфере здравоохранения в РФ как с точки зрения задач, которые они должны решать, так и требований, которые к ним предъявляются.

В частности, «Требования к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций» предусматривают, что информация, содержащаяся в этих типах систем, подлежит защите в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации и законодательством Российской Федерации в области персональных данных.

Программно-технические средства «данных информационных систем должны:

а) располагаться на территории Российской Федерации;

б) соответствовать требованиям, предусмотренным постановлением Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»;

в) быть сертифицированными Федеральной службой безопасности Российской Федерации и (или) Федеральной службой по техническому и экспортному контролю в отношении входящих в их состав средств защиты информации, включающих программно-аппаратные средства, средства антивирусной и криптографической защиты информации и средства защиты информации от несанкционированного доступа, уничтожения, модификации и блокирования доступа к ней, а также от иных неправомерных действий в отношении такой информации (в том числе сведения, составляющие врачебную тайну);

г) обеспечивать хранение медицинской документации в форме электронных документов, предусматривая резервное копирование медицинской документации в форме электронных документов и метаданных, восстановление медицинской документации в форме электронных документов и метаданных из резервных копий;

д) обеспечивать протоколирование и сохранение сведений о предоставлении доступа и о других операциях с документами и метаданными в автоматизированном режиме, а также автоматизированное ведение электронных журналов учета точного времени и фактов размещения, изменения и удаления информации, содержания вносимых изменений;

е) функционировать в бесперебойном круглосуточном режиме, за исключением установленных периодов проведения работ по обслуживанию информационных систем и устранению неисправностей в работе, суммарная длительность которых не должна превышать 4 часов в месяц (за исключением перерывов, связанных с обстоятельствами непреодолимой силы);

ж) обеспечивать размещение информации в единой государственной информационной системе в сфере здравоохранения;

з) обеспечивать информационное взаимодействие информационных систем между собой путем обмена

информационными сообщениями посредством формирования, отправки, получения, обработки запросов и ответов, форматы которых разрабатываются операторами информационных систем в сфере здравоохранения на основе справочников и классификаторов, содержащихся в федеральном реестре нормативно-справочной информации в сфере здравоохранения;

и) формировать электронные подписи в автоматическом режиме и включать их в информационные сообщения, проверять содержащиеся в информационных сообщениях электронные подписи организаций и (или) их должностных лиц, в том числе организаций, являющихся операторами информационных систем, участвующих в информационном взаимодействии;

к) обеспечивать достоверность и актуальность сведений о медицинских организациях и медицинских работниках посредством информационного взаимодействия с федеральным реестром медицинских организаций, федеральным регистром медицинских работников Единой системы;

л) обеспечивать возможность ведения медицинской документации в форме электронных документов» [7].

В то же время ст. 91 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» создавала некоторую правовую неопределенность для реализации сформировавшихся механизмов обеспечения информационной безопасности. Ч. 5 и 6 этой статьи предусматривают для информационного обеспечения здравоохранения в РФ существование и иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг. Однако эти иные информационные системы не входят в состав информационных систем в сфере здравоохранения, а могут только к ним подключаться в порядке, на условиях и в соответствии с требованиями, установленными в настоящее время постановлением Правительства РФ от 12.04.2018 № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями». В результате возникла правовая ситуация, когда, с одной стороны, существуют определенные законом типы информационных систем в сфере здравоохранения и требования к ним, а, с другой стороны, есть иные информационные системы, которые по своей сути обеспечивают те же самые процессы, но на них данная регламентация не распространяется, если они находятся вне взаимодействия с информационными системами в здравоохранении.

На наш взгляд, эта правовая коллизия получила свое разрешение в связи с принятием в нашей стране Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в основе которого применительно к рассматриваемому нами вопросу положен не субъектный, а деятельностный подход.

Как хорошо известно, Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» распространяется только на субъекты критической информационной инфраструктуры (КИИ).

Согласно ст. 2 данного федерального закона субъекты критической информационной инфраструктуры – это государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления (АСУ), функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [8].

В «Методических рекомендациях по категорированию объектов критической информационной инфраструктуры сферы здравоохранения», утвержденных Министерством здравоохранения РФ 5 апреля 2021 г., дано разъяснение, что «для целей категорирования объектов критической информационной инфраструктуры под «иным законным основанием» понимается передача прав пользования информационными системами, информационно-телекоммуникационными сетями, АСУ на основании правовых актов или решений собственника без передачи права собственности на них. Например, на основании договора безвозмездного пользования, договора на право хозяйственного ведения, договора на право оперативного управления» [9].

В качестве основы для определения области деятельности в сфере здравоохранения выступает «Общероссийский классификатор видов экономической деятельности», утвержденный приказом Росстандарта от 31.01.2014 № 14-ст. Все, что перечислено в ОКВЭД под кодом 86, относится к видам деятельность в области здравоохранения [10].

Для квалификации наличия или отсутствия информационных систем или информационно-телекоммуникационных сетей, как необходимого условия для признания субъектом КИИ, будет вполне достаточно обращения к нормативным определениям этих понятий в ст. 2 в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите

информации». Для законодателя информационная система – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, где информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов, а информационно-телекоммуникационная сеть – это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [2].

В ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» дается нормативное определение АСУ, к котором под АСУ понимается «комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами» [8].

Если есть в наличии все эти необходимые условия, определяющие принадлежность к статусу субъекта КИИ, то имеются достаточные основания для применения требований, связанных с регламентацией медицинской деятельности на основе федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». Офтальмология здесь не будет исключением: информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, как объектов КИИ, должны получить информационную защиту.

ЗАКЛЮЧЕНИЕ

Таким образом, рассмотрение заявленной в статье темы неизбежно может иметь только общий характер в отношении медицинской деятельности в целом, так как российское законодательство не настолько специализировано, чтобы применительно к офтальмологии у нас была бы одна нормативно-правовая база, регламентирующая деятельность территориально распределенных информационных систем, а в отношении, например, кардиологии – уже была бы совсем другая. Очевидно, что это не случайно: везде применяется фактически одна и та же технологическая база.

Наличие всех необходимых условий, определяющих принадлежность к статусу субъекта КИИ, создает достаточные основания для применения требований, связанных с регламентацией медицинской деятельности на основе Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

ЛИТЕРАТУРА/REFERENCES

1. Lieto A. Cognitive design for artificial minds. London, UK: Routledge, Taylor & Francis, 2021.

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». [Federal Law No. 149-FZ of July 27, 2006 «On Information, Information Technologies and Information Protection». (In Russ.)]

3. Миняев А.А., Красов А.В., Сахаров Д.В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных. Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020;1: 29–33. [Minyaev AA, Krasov AV, Sakharov DV. A method for evaluating the effectiveness of the information protection system of geographically distributed personal data information systems. Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tekhnologii i dizaina. Seriya 1: Estestvennye i tekhnicheskie nauki. 2020;1: 29–33. (In Russ.)]

4. Костарев С.В., Липатников В.А., Сахаров Д.В. Модель процесса передачи результатов аудита и контроля в автоматизированной системе менеджмента предприятия интегрированной структуры. Проблемы информационной безопасности. Компьютерные системы. 2015;2: 120–125. [Kostarev SV, Lipatnikov VA, Sakharov D.V. A model of the process of transferring audit and control results in an automated enterprise management system of an integrated structure. Information Security Problems. Computer Systems. 2015;2: 120–125. (In Russ.)]

5. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). [The Constitution of the Russian Federation (adopted by popular vote on 12.12.1993 with amendments approved during the all-Russian vote on 01.07.2020). (In Russ.)]

6. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации». [Federal Law No. 323-FZ of 21.11.2011 «On the basics of public health protection in the Russian Federation. (In Russ.)]

7. Требования к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций, утвержденные приказом Министерства здравоохранения РФ от 24 декабря 2018 г. № 911н. [Requirements for state information systems in the field of healthcare of the subjects of the Russian Federation, medical information systems of medical organizations and information systems of pharmaceutical organizations, approved by Order of the Ministry of Health of the Russian Federation dated December 24, 2018 No. 911n. (In Russ.)]

8. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». [Federal Law No. 187-FZ of July 26, 2017 «On the security of the critical information infrastructure of the Russian Federation». (In Russ.)]

9. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения, утвержденные Министерством здравоохранения РФ 5 апреля 2021 г. [Methodological recommendations for categorizing objects of critical information infrastructure in the healthcare sector, approved by the Ministry of Health of the Russian Federation on April 5, 2021. (In Russ.)]

10. Общероссийский классификатор видов экономической деятельности, утвержденный приказом Росстандарта от 31.01.2014 № 14-ст. [The All-Russian classifier of types of economic activity approved by the order of Rosstandart dated 31.01.2014 No. 14-art. (In Russ.)]

Информация об авторах
Дмитрий Владимирович Сахаров, к.т.н., доцент, sguard7@mail.ru, https://orcid.org/0000-0002-6130-5321
Андрей Иванович Пешков, к.ф.н., доцент, ap2000@yandex.ru, https://orcid.org/0000-0003-3168-4006

Information about the authors
Dmitrii V. Sakharov, PhD in Engineering, Associate Professor, sguard7@mail.ru, https://orcid.org/0000-0002-6130-5321

Andrei I. Peshkov, PhD in Philosophy, Associate Professor, ap2000@yandex.ru, https://orcid.org/0000-0003-3168-4006

Вклад авторов в работу:
Д.В. Сахаров: существенный вклад в концепцию и дизайн работы, сбор, анализ и обработка материала, написание текста, редактирование, окончательное утверждение версии, подлежащей публикации.
А.И. Пешков: существенный вклад в концепцию и дизайн работы, сбор, анализ и обработка материала, написание текста.

Authors' contribution:
D.V. Sakharov: significant contribution to the concept and design of the work, collection, analysis and processing of material, writing, editing, final approval of the version to be published.
A.I. Peshkov: significant contribution to the concept and design of the work, collection, analysis and processing of material, writing.

Финансирование: Авторы не получали конкретный грант на это исследование от какого-либо финансирующего агентства в государственном, коммерческом и некоммерческом секторах.

Согласие пациента на публикацию: Письменного согласия на публикацию этого материала получено не было. Он не содержит никакой личной идентифицирующей информации.
Конфликт интересов: Отсутствует.

Funding: The authors have not declared a specific grant for this research from any funding agency in the public, commercial or not-for-profit sectors.
Patient consent for publication: No written consent was obtained for the publication of this material. It does not contain any personally identifying information.
Conflict of interest: There is no conflict of interest.

Поступила: 14.11.2022
Переработана: 21.11.2022
Принята к печати: 16.12.2022

Originally received: 14.11.2022
Final revision: 21.11.2022
Accepted: 16.12.2022