https://doi.org/10.29188/2712-9217-2021-7-4-48-57

Защита персональных данных пациентов при использовании телемедицинских технологий в период пандемии COVID-19

Литературный обзор

Д.М. Монаков[1,2], В.А. Шадеркина[3], С.А. Рева[4,5], А.А. Грицкевич[2,6]

[1] ГКБ им. С. П. Боткина; д. 5, 2-й Боткинский пр., Москва, 125284, Россия
[2] Российский университет дружбы народов, кафедра урологии и оперативной нефрологии с курсом онкоурологии; д. 6, ул. Миклухо-Маклая, Москва, 117198, Россия
[3] Урологический информационный портал UroWeb.ru; д. 11, ул. Золотая, Москва, 105094, Россия
[4] ФГБОУ ВО «ПСПбГМУ им. И.П. Павлова», НИЦ урологии; д. 17, ул. Льва Толстого, Санкт-Петербург, 197101, Россия
[5] ФГБУ «НМИЦ онкологии имени Н.Н. Петрова», отделение онкоурологии; д. 68, ул. Ленинградская, пос. Песочный, Санкт-Петербург, 197758, Россия
[6] ФГБУ «Национальный медицинский исследовательский центр хирургии им. А.В. Вишневского» Минздрава России; д. 27, ул. Большая Серпуховская, Москва, 117997, Россия

Контакт: Монаков Дмитрий Михайлович, gvkg-monakov@mail.ru

Аннотация:

Ведение. Пандемия новой коронавирусной инфекции способствовала дальнейшему развитию информационных, в том числе, телемедицинских технологий, а также привлекла внимание общества к целому ряду связанных с ними проблем, требующих скорейшего решения. Одна из них – защита персональных данных. Настоящий литературный обзор был предпринят нами для систематизации имеющейся сведений по данному вопросу.
Материалы и методы. Проведен поиск публикаций в базах данных PubMed, e-Library, Google Scholar, «Гарант», «Консультант» и на официальных сайтах государственных учреждений Российской Федерации с использованием ключевых слов «персональные данные», «телемедицина», «защита», «угрозы», «personal data», «security», «threats», «telemedicine». В результате найдено 43 публикации, которые включены в настоящий обзор.
Результаты. В обзоре приведены основные понятия, связанные персональными данными, перечислены типы угрозы для них и уровни защищенности, систематизированы мероприятия по обеспечению защиты персональных данных и приведена их краткая характеристика. Также очерчены особенности сбора, обработки, хранения и использования персональных данных при использовании телемедицинских технологий.
Обсуждение. Сбор персональных данных может проводиться с административными, научными, коммерческими или криминальными целями. Появление современных технологий «big data» значительно облегчило процесс сбора и обработки данных, а также доступ к ним, но также повысило их уязвимость. Процесс защиты информации требует комплексного применения различных правовых, организационных и технических мероприятий, что требует значительных финансовых, материальных и временных затрат. Для рационального использования ресурсов информацию, требующую защиты, группируют по уровням защищенности, которые определяются категорией, характеристикой данных и типом угроз для них.
Выводы. Существующие на сегодняшний день законодательные принципы регулирования в этой области значительно отстают от стремительного развития технологий, что требует фундаментального их пересмотра. На сегодняшний день ведущая роль в обеспечении безопасности персональных данных принадлежит организационным и техническим мероприятиям.

Ключевые слова: персональные данные; телемедицина; защита; угрозы.

Для цитирования: Монаков Д.М., Шадеркина В.А., Рева С.А., Грицкевич А.А. Защита персональных данных пациентов при использовании телемедицинских технологий в период пандемии COVID-19. Российский журнал телемедицины и электронного здравоохранения 2021;7(4):48-57; https://doi.org/10.29188/2712-9217-2021-7-4-48-57

Protection of personal data of patients when using telemedicine technologies during the COVID-19 pandemic

Literature review

https://doi.org/10.29188/2712-9217-2021-7-3-48-57

D.M. Monakov[1,2], V.A. Shaderkina[3], S.A. Reva[4,5], A.A. Gritskevich[2,6]

[1] Clinical hospital named after S.P. Botkin; 5, 2nd Botkinsky pr, Moscow, 125284, Russia
[2] Peoples' Friendship University of Russia, Department of Urology and Operative Nephrology with a course on urology; 6, st. Miklukho-Maklaya, Moscow, 117198, Russia
[3] Urological information portal UroWeb.ru; 11, st. Zolotaya, Moscow, 105094, Russia
[4] Pavlov First Saint Petersburg State Medical University, Research Institute of Urology; 17 Lev Tolstoy street, Saint Petersburg, 197101, Russia
[5] N.N. Petrov Research Institute of Oncology, Department of oncourology; 68 Leningradskaya street, Pesochny, Saint Petersburg, 197758, Russia
6 A.V. Vishnevsky National Medical Research Center of Surgery; 27, Bolshaya Serpukhovskaya str., Moscow, 117997, Russia

Contact: Dmitry M. Monakov, gvkg-monakov@mail.ru

Summary:

Introduction. The pandemic of COVID-19 has promoted the development of information and telemedicine technologies but also has risen some questions about their challenges. One of them is the secure of personal data. This review is aim to discuss those issues.
Materials and methods. We have sought publications in the databases PubMed, e-Library, Google Scholar, Guarantor, Consultant and on the official websites of Russian state institutions using the keywords «personal data», «telemedicine», «protection», «threats», «personal data», «security», «threats», «telemedicine». Forty three publications were found and included in this review.
Results. The review presents the basic concepts related to personal data, lists the types of threats to them and the levels of security, systematizes measures to ensure the protection of personal data and provides a brief description of them. The features of the collection, processing, storage and use of personal data when using telemedicine technologies are also outlined.
Discussion. Personal data may be collected for administrative, scientific, commercial or criminal purposes. The emergence of modern "big data" technologies has greatly facilitated the process of data collection and processing, as well as access to them, but also increased their vulnerability. The process of information protection requires the complex application of various legal, organizational and technical measures, which requires significant financial, material and time costs. For the rational use of resources, information requiring protection is grouped by security levels, which are determined by the category, characteristics of the data and the type of threats to them.
Conclusions. The current legislative principles of regulation in this area are significantly lagging behind the rapid development of technologies, which requires a fundamental revision of them. To date, the leading role in ensuring the security of personal data belongs to organizational and technical measures.

Key words: personal data; telemedicine; protection; threats.

For citation: Monakov D.M., Shaderkina V.A., Reva S.A., Gritskevich A.A. Protection of patients' personal data when using telemedicine technologies during the COVID-19 pandemic. Russian Journal of Telemedicine and E-Health 2021;7(4):48-57; https://doi.org/10.29188/2712-9217-2021-7-4-48-57

ВВЕДЕНИЕ

Пандемия новой коронавирусной инфекции COVID-19 способствовала дальнейшему развитию различных информационных технологий, которые в последние десятилетия неизбежно становятся частью нашей жизни.

Не стала исключением и телемедицина, которая позволила смягчить последствия тех ограничений, которые система здравоохранения была вынуждена ввести при оказании некоторых видов медицинской помощи в первой половине 2020 года. Массовое использование гражданами мобильных устройств в период «самоизоляции» дало возможность отслеживать их местонахождение и контакты, что проводилось в целях оперативного сбора информации о распространении заболевания, однако привело к выраженной негативной реакции общества на данные действия, очередной раз обострив вопрос о защите персональных данных [1].

Согласно действующему российскому законодательству к персональным данным относится любая информация, которая прямо или косвенно относится к физическому лицу – субъекту персональных данных, т. е. к этой категории можно отнести достаточно большой объем различных сведений [2].

Важно отметить, что проводимая на основе использования персональных данных идентификация личности пациента, а также принадлежности к нему сведений, полученных в ходе обследования, и назначенного лечения – ключевой аспект безопасности медицинской деятельности, поэтому ее осуществление без сбора такой ▸▸

информации невозможно. В связи этим проблема защиты персональных данных в области телемедицины на сегодняшний день остается чрезвычайно актуальной.

Цель настоящего литературного обзора – систематизация имеющихся на сегодняшний день сведений о защите персональных данных при использовании телемедицинских технологий, а также поиск возможных путей решения проблем в данной области.

МАТЕРИАЛЫ И МЕТОДЫ

Проведен поиск, анализ и систематизация публикаций в базах данных PubMed, e-Library, Google Scholar, «Гарант», «Консультант» и на официальных сайтах государственных учреждений Российской Федерации с использованием ключевых слов «персональные данные», «телемедицина», «защита», «угрозы», «personal data», «security», «threats», «telemedicine». Также проведен поиск дополнительных источников в пристатейных списках литературы. Тезисы конференций и симпозиумов, а также диссертации и их авторефераты исключены. В результате найдено 43 публикации, которые включены в настоящий обзор.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Понятие персональных данных

Сбор различной информации о личности проводился на протяжении всей истории человечества. Еще с древнейших времен с целью налогообложения или воинского учета осуществлялись переписи населения, которые, по сути, были сбором персональных данных.

Следует подчеркнуть, что накопление любых сведений всегда осуществляется с определенными *целями*, среди которых можно выделить четыре группы [2].

Первая – административные. Их основная задача – получение информации, необходимой для принятия различных управленческих решений. Это налогообложение, воинский учет, регистрация актов гражданского состояния, образовательная деятельность, страховое и банковское дело, работа кадровых органов, медицина и др.

Ко ***второй группе*** относятся научные цели, при которых сбор персональных данных осуществляется с целью разработки и проверки научных гипотез.

Третья группа – коммерческие цели. Это изучение профиля потребителя для продвижения товаров и услуг, проведения рекламных кампаний, анализ рынков сбыта и т. п.

Четвертую группу составляют криминальные цели (мошенничество, шантаж или иное нанесение ущерба личности за счет использования, уничтожения или изменения его персональных данных).

Эти цели определяют объем и характер собираемых данных, которые должны быть достоверными и полными (достаточными для достижения целей).

В процессе истории человечества цели сбора персональных данных, который проводился государством, а также различными организациями и частными лицами, постоянно менялись. Это приводило к изменению характера интересующей их информации, а ее объем неизменно увеличивался.

По данным экспертов в 2017 г. общее количество хранящейся в мире информации составляло 16,2 зеттабайта, а по прогнозам аналитиков оно будет увеличиваться вдвое каждые 2 года и к 2025 г. составит около 163,0 зеттабайта. Такое драматическое увеличение объема данных из различных источников потребовало разработки новых методик и технологий, которые получили название «большие данные» («Big Data») [3]. Их определяющие характеристики («три V»):

- объем (Volume) – огромные физические объемы данных;
- многообразие (Variety) – одновременное накопление разных видов и типов данных;
- скорость (Velocity) – большая скорость прироста и обработки данных [4].

Появление современных технологий значительно облегчило процесс сбора, систематизации, хранения и анализа данных, а также доступ к ним, что критически повысило их ценность в современном мире, но вместе с тем, сделало их более уязвимыми.

Информация стала «товаром», «материальной ценностью» и, следовательно, потребовала защиты [3, 5].

Первый в мире закон о защите персональной информации был принят в 1970 г. в ФРГ, земля Гессен. А уже в 1977 г. подобный закон был принят в Германии на федеральном уровне [5].

В 1981 году Советом Европы была принята Конвенция о защите физических лиц при автоматизированной обработке персональных данных [6].

Конституция Российской Федерации, принятая в 1993 г., запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия [7].

Конвенция СЕ от 1981 г. ратифицирована Россией в 2005 г., после чего последовало принятие в 2006 г. Федерального закона «О персональных

данных», который отражает принципы защиты и обработки подобных сведений, принятые в европейских странах [2, 3, 8].

Угрозы для персональных данных

Персональные данные могут быть подвержены различным угрозам, под которыми понимают совокупность условий и факторов, которые создают опасность несанкционированного, в том числе случайного доступа к ним при хранении или в процессе обработки в информационной системе, результатом чего могут стать те или иные неправомерные действия [9].

В соответствии с действующим законодательством любой государственный (муниципальный) орган, а также юридическое или физическое лицо, осуществляющее сбор, обработку и хранение персональных данных, называется оператором. Обработкой персональных данных считаются любые действия, совершаемые с ними [2].

В зависимости от цели, которую преследует оператор персональных данных, и его функциональных обязанностей, он может быть регистратором, который собирает данные и вводит их в базу данных, пользователем, которому эта информация необходима для осуществления своей профессиональной деятельности (например, врач, медицинская сестра, исследователь и др.), или относиться к «техническому персоналу», чья функция заключается в непосредственной работе с данными, например, их обезличивание, кодирование, систематизация (например, IT-специалист). Выделение таких категорий операторов представляется существенным для организации защиты персональных данных [3].

При работе с персональными данными можно выделить следующие этапы:

- сбор информации и ее введение в базу данных регистратором на основании сведений, представленных носителем персональных данных или полученных иным путем;
- обработка (систематизация, обезличивание и т. п.);
- хранение на носителе информации (сервере);
- доступ к ним пользователей;
- передача персональных данных пользователям, не имеющих прямого доступа к ним, а также обмен ими между различными базами данных.

В процессе этих действий могут возникнуть следующие угрозы для персональных данных:

- ошибка или намеренное искажение информации при ее введении в базу данных;
- утрата (хищение) информации на этапе ввода или хранения вследствие несанкционированного (преднамеренного или случайного) доступа к ней посторонних лиц;
- уничтожение (полное или частичное), искажение (модификация данных, нарушающая их достоверность) информации, блокирование доступа к ней при ее хранении или передаче вследствие злонамеренных действий какого-либо лица, технического сбоя или ошибки оператора.

В законодательстве выделяют также и другие угрозы – копирование, предоставление, распространение, однако, на наш взгляд эти действия могут считаться следствием хищения персональных данных, детализация последствий которого не существенна.

Меры по защите персональных данных

Наличие актуальных угроз для персональных данных требует проведения мероприятий по их защите, под которой подразумевается деятельность, направленная на предотвращение несанкционированного и непреднамеренного (например, ошибка пользователя, сбой технического или программного обеспечения) воздействия на них. Такие мероприятия могут быть правовыми (регламентирующими, надзорными, карательными), техническими (использование программно-технических средств для решения задач по защите данных), криптографическими (кодирование информации) и физическими (организационные мероприятия, предусматривающие введение режимных, временных, территориальных и пространственных ограничений). Эти мероприятия должны быть комплексными и непрерывными, потому они применяются в рамках системы защиты информации, которая представляет собой совокупность органов (исполнителей), используемой ими техники и объектов защиты информации. К последним относят не только саму информацию, но ее носители и информационные процессы, а также помещения, здания и территорию, где осуществляется обработка данных [9, 10].

В соответствии с действующим законодательством обязанность по защите персональных данных лежит на их операторе [2, 10].

В информационных системах выделяют три типа угроз для персональных данных (табл. 1) [10].

В связи с неоднородностью персональных данных, различными по своей тяжести последствиями их утраты или изменения, а также сложностью их защиты, которая к тому же требует значительных материальных затрат, все мероприятия по ▸▸

предотвращению угроз для них разделены на четыре уровня (от 1 – наивысшего, до 4 – низшего). Они определяются типом угроз, категорией персональных данных и характеристикой их субъектов (табл. 2) [10].

Такая классификация типов угроз для персональных данных и стратификация уровней их защищенности позволяет рационально использовать ресурсы, необходимые для осуществления мероприятий по их защите. Основные мероприятия по обеспечению безопасности персональных данных представлены в таблице 3 [10].

Принципиальное отличие информационных медицинских технологий состоит в том, что при их использовании помимо данных о личности пациента (фамилия, имя, отчество, дата рождения, адрес проживания, паспортные данные и т.п.) проводится постоянный сбор и хранение информации о состоянии его здоровья в виде электронной истории болезни [11].

Для электронных медицинских записей выделяют следующий «жизненный цикл»:

- создание записи;
- ее ведение;
- подписание;
- хранение информации с предоставлением доступа к ней заинтересованных лиц;
- уничтожение записи [11].

Таблица 1. Типы угроз для персональных данных
Table 1. Types of threats for personal data

Тип угроз / Threats type	Характеристика / Features
1	Связаны с возможностями системного программного обеспечения Threats related to system software opportunities
2	Связаны с возможностями прикладного программного обеспечения Threats related to application software opportunities
3	Связаны с причинами, не относящимися к программному обеспечению Threats not related to software

Таблица 2. Уровни защищенности персональных данных
Table 2. Security levels for personal data

Уровень защищенности / Security level	Условия применения / Conditions for use								
	Тип угроз Threats type			Категория данных Data's categories				Характеристика субъектов персональных данных Personal data subjects' features	
	1	2	3	С	Б	О	И	Работники оператора ПД Employees of personal data operator	Количество Number
1	+			+	+		+		
		+		+					> 100 000
2	+					+			
		+		+				+	< 100 000
		+			+				
		+				+			> 100 000
		+					+		> 100 000
			+	+					> 100 000
3		+				+		+	> 100 000
		+					+	+	> 100 000
			+	+				+	> 100 000
			+		+				
			+				+		> 100 000
4			+			+			
			+				+	+	> 100 000

Примечания:
С – специальные персональные данные (сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни);
Б – биометрические персональные данные (сведения о физиологических и биологических особенностях человека, на основании которых можно установить его личность);
О – общедоступные персональные данные сведения, которые может получить неограниченный круг лиц, например, из открытых для общего пользования источников (фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и т. п.);
И – иные сведения.
Notes:
С – special personal date (race, nationality, politic, religious or philosophic beliefs, health status, sexual life);
Б – biometric personal data (information about physiological and biological features of individual which make possible his or her identification);
О – publicly available personal data (name, date and place of birth, address, telephone number, occupation and over information which can be available for wide range of people from open sources);
И – other data about person.

Таблица 3. Мероприятия по обеспечению безопасности персональных данных
Table 3. Personal data security measures

Уровень защищенности / Security level	Мероприятия по обеспечению безопасности Security measures
4	Ограничение доступа посторонних лиц в помещения, где находится оборудование информационной системы Restriction of unauthorized persons access to the premises with information system equipment
	Обеспечение сохранности носителей данных Ensuring the safety of data carriers
	Утверждение списка работников оператора, которым разрешен доступ к обрабатываемым персональным данным Approval of the list of employees of the operator who are allowed access to the processed personal data
	Использование программно-технических средств защиты информации Use of software and technical means of information protection
3	Выполнение требований, предусмотренных для четвертого уровня защищенности данных Accomplishment of forth level measures
	Назначение должностного лица, ответственного за обеспечение безопасности данных в информационной системе Appointment of an official responsible for ensuring data security in the information system
2	Выполнение требований, предусмотренных для третьего уровня защищенности данных Accomplishment of third level measures
	Ограничение доступа к электронному журналу безопасности исключительно уполномоченными лицами Restriction of access to the electronic security log exclusively by authorized persons
1	Выполнение требований, предусмотренных для второго уровня защищенности данных Accomplishment of second level measures
	Обеспечение автоматической регистрации в электронном журнале безопасности изменений полномочий сотрудника оператора по доступу к данным, содержащимся в информационной системе Ensuring automatic registration in the electronic security log of changes in the operator's employee's authority to access data contained in the information system
	Создание структурного подразделения, ответственного за обеспечение безопасности данных в информационной системе или возложение данных обязанностей на уже существующее структурное подразделение Creating a structural unit responsible for ensuring data security in an information system or assigning these responsibilities to an existing structural unit

Создание электронной медицинской записи – это процесс первичной регистрации пациента в информационной системе.

При использовании медицинских технологий пациент может самостоятельно вносить свои персональные данные при регистрации на портале, через который осуществляется данный вид деятельности, или же это производится уполномоченным на это медицинским работником.

Электронная история болезни – это динамичный документ, который постоянно дополняется, отражая изменения состояния здоровья пациента. Записи в ней выполняются врачами, но при использовании телемедицинских технологий это может делать и сам пациент, например, загружая в систему данные своего обследования. Чтобы такая запись получила статус официального документа, она должна быть создана уполномоченным на это лицом, идентифицированным при входе в систему с помощью специальных технологий и подписано им [12, 13].

Перечень сотрудников, допущенных к работе с электронными медицинскими записями, а также их права на действия с ними определяет руководство медицинского учреждения, работающего в системе телемедицины, которое также осуществляет контрольные мероприятия [14].

Исполнение данных управленческих решений проводится с использованием программно-технического обеспечения (пароли, электронная подпись, автоматическая регистрация действий в системе, сигнализация о нарушениях и т. п.) [15, 16].

Одной из ключевых задач при работе с персональными данными остается обеспечение их защиты в процессе хранения [17]. Это может быть достигнуто с помощью их обезличивания, что обеспечивается [18]:

- введением идентификаторов – заменой персональных данных специальными символами с созданием каталогов их соответствия исходным записям;
- изменением состава или семантики данных – заменой информации результатами ее статистической обработки, объединением или исключением части сведений;
- декомпозицией – разделением множества персональных данных конкретных субъектов на подмножества с дальнейшим их обособленным хранением;
- перемешиванием – перемещением и перестановкой отдельных записей в множестве персональных данных конкретных субъектов.

После проведения процедуры обезличивания персональные данные должны сохранять свою полноту, структурированность и семантическую ценность, приобретая при этом анонимность [18]. Следует отметить, что наличие современных технологий («Big Data») позволяет проведение ▸▸

деобезличивания, что ставит под вопрос эффективность и целесообразность этого метода [19, 20].

Использование телемедицинских технологий подразумевает постоянный обмен информацией в режиме «клиент-сервер» через интернет по стандартному протоколу TCP/IP, что наиболее выгодно с экономической точки зрения. Однако это повышает ее уязвимость в процессе передачи данных [21]. При хранении и передаче информации применяются различные средства ее криптографической защиты [22]. Технические средства обеспечения защиты информации обеспечивают девять классов защищенности информации от несанкционированного доступа к ней. Каждый из них характеризуется определенным минимальным набором требований к защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации [23].

Система защиты информации должна состоять из четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности [23].

Все оборудование, используемое с данной целью должно проходить обязательную государственную сертификацию [24].

Прикладная область информатики, занимающаяся вопросами обеспечения безопасности данных, носит название DLP (Data Loss/Leakage Prevention). Специалисты в данной области выделяют два канала утечки информации – сеть и мобильные носители данных. Ее причинами могут быть следующие факторы: внешние (DoS-атака), внутренние (умышленные и неумышленные действия сотрудников) и смешанные (внедрение вредоносного программного обеспечения через Web-браузеры или спам). До 90% причин утечек – внутренние.

Специалисты в данной области признают, что обеспечить абсолютную защиту данных невозможно, поэтому вся деятельность в этом направлении сводится к максимальному снижению рисков.

Ими предложено три подхода к созданию DLP-систем: 1) анализ контента (содержания получаемой и передаваемой информации) по специальному алгоритму с использованием ключевых слов; 2) грифование электронных документов специальными метками; 3) комбинация этих подходов [25, 26].

Важным моментом, на который обращают внимание специалисты, занимающиеся проблемами обеспечения безопасности персональных данных при использовании телемедицинских технологий, это требование к хранению данных о состоянии здоровья граждан исключительно на внутренних серверах государства [27].

Одной из нерешенных проблем остается задача идентификации личности сторон процесса обмена информацией, что создает сложности с обеспечением конфиденциальности данного процесса [28, 29].

Существующее правовое регулирование деятельности в рамках телемедицинских технологий не соответствует требованиям этой динамично развивающейся отрасли и создает для нее необоснованные барьеры [30–32].

Появлению любого правового документа предшествует прецедент, то есть значимое для общества событие. После осознания проблемы и выдвижения законодательных инициатив следует их длительное обсуждение и выполнение необходимых процедур, необходимых для принятия правовых актов. Все это приводит к тому, что законодательное регулирование, как правило, запаздывает, создавая на протяжении определенного времени «правовой вакуум» или не отвечает стремительно изменяющимся потребностям общества.

Одним из примеров может служить требование получения информированного согласия на обработку персональных данных.

В настоящее время в Российской Федерации существует презумпция несогласия лица на любые действия с его персональными данными. Так, в соответствии с п. 8 ст. 10.1 Закона о персональных данных молчание или бездействие субъекта таких сведений ни при каких обстоятельствах не может считаться согласием на их обработку. Правда этот же Закон оговаривает особые случаи, к которым относят в том числе обработку данных в целях защиты жизни и здоровья граждан, при оказании медицинской помощи, в области обязательных видов страхования, проведении научных исследований [2].

В процессе работы любой медицинской организации регулярно возникает необходимость сбора персональных данных и обязательной передачи их в страховую организацию [33].

Закон о персональных данных требует от оператора заранее определять перечень персональных данных, цели их накопления и способы обработки. Однако реализация потенциала телемедицинских технологий не всегда предполагает возможность выполнения этих требований. Таким образом, наиболее инновационная сфера телемедицины остается за пределами правового регулирования [34].

По мере развития информационных технологий соблюдение требований к информированному согласию становится исключительно фор-

мальным и не обеспечивает подлинной реализации прав гражданина [35]. Тем более, что при осуществлении медицинской деятельности действующее законодательство в любом случае требует соблюдения врачебной тайны [36].

При использовании телемедицинских технологий получение информированного согласия технически сложно, а информация, запрашиваемая у субъекта персональных данных при его подписании явно избыточная [30].

Именно поэтому в настоящее время назрела острая необходимость пересмотра законодательных требований к получению согласия на сбор и обработку персональных данных. Их следует дифференцировать в зависимости от цели оператора. Например, при сборе таких сведений с административными целями (в том числе, при оказании медицинской помощи) целесообразно вовсе отказаться от его получения. Это приведет к существенной экономии ресурсов (как материальных, так и временных), а также снизит беспокойство граждан, у которых процедура получения такого согласия часто вызывает большее беспокойство, чем сама возможность сбора сведений об их личности. В ряде случаев (например, при сборе персональных данных с исследовательскими целями) целесообразно осуществление этого процесса без согласия гражданина, до тех пор, пока субъект не выразит несогласия (модель «opt-out»). Сбор персональных данных с коммерческой целью следует проводить только с согласия гражданина [30].

При разрешении законодательных проблем в этой области возможно два пути: ситуативный – внесение исключений в действующее законодательство и фундаментальный, который предусматривает пересмотр его принципов. Если первый подход позволяет оперативно реагировать на выявленные проблемы, то последний более предпочтителен в долгосрочной перспективе [30].

ВЫВОДЫ

Стремительное развитие информационных технологий неизбежно охватывает практически все аспекты жизнедеятельности современного человека, в том числе, медицину.

Абсолютное большинство российских врачей готово к применению телемедицинских технологий в своей повседневной деятельности [37]. Их правовой статус уже закреплен на законодательном уровне [38–42].

Телемедицина – одно из наиболее динамично развивающихся направлений, в связи с чем не прекращается дискуссия по многим ее аспектам [43].

Защита персональных данных при использовании телемедицинских технологий остается одним из наиболее болезненных вопросов, поскольку информация о состоянии здоровья граждан требует обеспечения наивысшего уровня защищенности.

Вместе с тем в реальной практике такие мероприятия часто носят формальный характер. Информированное согласие на сбор и обработку персональных данных не обеспечивает прав пациента на конфиденциальность личной жизни и соблюдение врачебной тайны.

Юридическая база, как правило, отстает от стремительного развития цифровых технологий и реагирует уже на состоявшиеся события, которые служат основой для разработки и принятия законодательных актов. Поэтому основу защиты персональных данных должны составлять организационные и технические мероприятия, способные обеспечить повышенные стандарты безопасности и динамично развиваться, своевременно реагируя на неизбежное появление новых угроз, бурное развитие информационных технологий и достижения медицинской науки.

ЛИТЕРАТУРА

1. Шахабов И.В., Мельников Ю.Ю., Смышляев А.В. Особенности развития цифровых технологий в здравоохранении в условиях пандемии COVID-19. *Научное обозрение. Медицинские науки* 2020;(6):66-71. [Shahabov I.V., Melnikov Yu.Yu., Smyishlyaev A.V. Osobennosti razvitiya tsifrovyih tehnologiy v zdravoohranenii v usloviyah pandemii COVID-19. *Nauchnoe obozrenie. Meditsinskie nauki = Scientific Review. Medical sciences* 2020;(6):66-71. (in Russian)].
2. Федеральный закон № 152-ФЗ от 27 июля 2006 г. (редакция от 2 июля 2021 г.) «О персональных данных». [Электронный ресурс]. (Дата обращения 4 августа 2021). URL: http://ivo.garant.ru/#/document/12148567/paragraph/22727:0. Federal Law # 152-FZ of 2006 July 27 (edition from 2021 July 02) «About the protection of personal data» [cited 2021 Aug 04]. Available from: http://ivo.garant.ru/#/document/12148567/paragraph/22727:0.(in Russian)].
3. Шайдуллина В.К. Большие данные и защита персональных данных: основные проблемы теории и практики правового регулирования. *Общество: политика, экономика, право* 2019;66(1):51-55. [Shaydullina V.K. Bolshie dannyie i zaschita personalnyih dannyih: osnovnyie problemyi teorii i praktiki pravovogo regulirovaniya. *Obschestvo: politika, ekonomika, pravo = Society: Politics, Economics, Law* 2019;66(1):51-55. (in Russian)].
4. Столяр В.П., Крайнюков П.Е., Калачев О.В. Цифровая трансформация здравоохранения и ведомственной медицины. М.: Планета, 2020;200 с. [Stolyar V.P., Kraynyukov P.E., Kalachev O.V. Tsifrovaya transformatsiya zdravoohraneniya i vedomstvennoy meditsinyi. M.: Planeta, 2020;200 s. (in Russian)].
5. Коровяковский Д.Г. Российский и зарубежный опыт защиты персональных данных. *Угрозы и безопасность* 2009;38(5):48-54. [Korovyakovskiy D.G. Rossiyskiy i zarubezhnyiy opyit zaschityi personalnyih dannyih. *Ugrozyi i bezopasnost = Threats and security* 2009;38(5):48-54. (in Russian)].
6. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г. с изменениями от 15 июня 1999 г.), ратифицирована в России Федеральным Законом от 19 декабря 2005 г. №160-ФЗ. [Электронный ресурс]. URL: https://pd.rkn.gov.ru/law/p131/document170.htm. [Konventsiya Soveta Evropyi o zaschite fizicheskih lits pri avtomatizirovannoy obrabotke personalnyih dannyih (Strasburg, 28 yanvarya 1981

ЛИТЕРАТУРА

g. s izmeneniyami ot 15 iyunya 1999 g.), ratifitsirovana v Rossii Federalnyim Zakonom ot 19 dekabrya 2005 g. #160-FZ. [Elektronnyiy resurs]. URL: https://pd.rkn.gov.ru/law/p131/document170.htm. (in Russian)].

7. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). [Электронный ресурс]. URL: http://ivo.garant.ru/#/document/10103000/paragraph/131:0 (Дата обращения 4 августа 2021) [cited 2021 Jul 04] Available from: http://ivo.garant.ru/#/document/10103000/paragraph/131:0. [Konstitutsiya Rossiyskoy Federatsii (prinyata vsenarodnyim golosovaniem 12.12.1993 g. s izmeneniyami, odobrennyimi v hode obscherossiyskogo golosovaniya 01.07.2020). [Elektronnyiy resurs]. URL: http://ivo.garant.ru/#/document/10103000/paragraph/131:0 (Data obrascheniya 4 avgusta 2021) [cited 2021 Jul 04] Available from: http://ivo.garant.ru/#/document/10103000/paragraph/131:0. (in Russian)].

8. Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных». [Электронный ресурс]. URL: https://54.rkn.gov.ru/protection/acts/?special=1. [Federalnyiy zakon ot 19.12.2005 # 160-FZ «O ratifikatsii konventsii Soveta Evropyi o zaschite fizicheskih lits pri avtomatizirovannoy obrabotke personalnyih dannyih». [Elektronnyiy resurs]. URL: https://54.rkn.gov.ru/protection/acts/?special=1. (in Russian)].

9. ГОСТ Р 50922-2006 «Защита информации: основные термины и определения». М.: Стандартинформ, 2008; 8 с. [GOST R 50922-2006 «Zaschita informatsii: osnovnyie terminyi i opredeleniya». M.: Standartinform, 2008; 8 s. (in Russian)].

10. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/ (Дата обращения: 4 августа 2021). [Postanovlenie Pravitelstva RF ot 01.11.2012 # 1119 «Ob utverzhdenii trebovaniy k zaschite personalnyih dannyih pri ih obrabotke v informatsionnyih sistemah personalnyih dannyih». [Elektronnyiy resurs]. URL: http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/ (Data obrascheniya: 4 avgusta 2021). (in Russian)].

11. ГОСТ Р 52636-2006 «Электронная история болезни. Общие положения»; М.: Стандартинформ, 2007; 20 с. [GOST R 52636-2006 «Elektronnaya istoriya bolezni. Obschie polozheniya»; M.: Standartinform, 2007; 20 s. (in Russian)].

12. Постановление Правительства РФ от 28.11.2011 г. № 977 (ред. от 24.06.2021) «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме». [Электронный ресурс]. URL: http://government.ru/docs/all/79841/. [Postanovlenie Pravitelstva RF ot 28.11.2011 g. # 977 (red. ot 24.06.2021) «O federalnoy gosudarstvennoy informatsionnoy sisteme «Edinaya sistema identifikatsii i autentifikatsii v infrastrukture, obespechivayuschey informatsionno-tehnologicheskoe vzaimodeystvie informatsionnyih sistem, ispolzuemyih dlya predostavleniya gosudarstvennyih i munitsipalnyih uslug v elektronnoy forme». [Elektronnyiy resurs]. URL: http://government.ru/docs/all/79841/. (in Russian)].

13. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи». [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/32938. [Federalnyiy zakon ot 06.04.2011 # 63-FZ «Ob elektronnoy podpisi». [Elektronnyiy resurs]. URL: http://www.kremlin.ru/acts/bank/32938. (in Russian)].

14. Назаров И. Г., Язов Ю. К., Остроухова Е. С. Особенности организации обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных. *Информация и безопасность* 2009;(1):71-76. [Nazarov I.G., Yazov Yu.K., Ostrouhova E.S. Osobennosti organizatsii obespecheniya bezopasnosti personalnyih dannyih pri ih obrabotke v informatsionnyih sistemah personalnyih dannyih. *Informatsiya i bezopasnost = Information and security* 2009(1):71-76. (in Russian)].

15. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». [Prikaz FSTEK Rossii ot 18.02.2013 # 21 «Ob utverzhdenii sostava i soderzhaniya organizatsionnyih i tehnicheskih mer po obespecheniyu bezopasnosti personalnyih dannyih pri ih obrabotke v informatsionnyih sistemah personalnyih dannyih». (in Russian)].

16. Полещук А.В. Основы защиты персональных данных. *Т-comm: Телекоммуникации и транспорт* 2009;3(5):44-47. [Poleschuk A.V. Osnovyi zaschityi personalnyih dannyih. *T-comm: Telekommunikatsii i transport = T-Comm* 2009;3(5):44-47. (in Russian)].

17. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702. [Prikaz FSTEK Rossii ot 11 fevralya 2013 g. # 17 «Ob utverzhdenii trebovaniy o zaschite informatsii, ne sostavlyayuschey gosudarstvennuyu taynu, soderzhascheysya v gosudarstvennyih informatsionnyih sistemah». [Elektronnyiy resurs]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702. (in Russian)].

18. Парфенов Н.П. Обезличивание персональных данных – эффективный способ защиты персональных данных сотрудников ОВД. В сборнике: Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления 2015:29-32. [ParfYonov N.P. Obezlichivanie personalnyih dannyih – effektivnyiy sposob zaschityi personalnyih dannyih sotrudnikov OVD. V sbornike: Regionalnaya informatika i informatsionnaya bezopasnost. Sbornik trudov. Sankt-Peterburgskoe Obschestvo informatiki, vyichislitelnoy tehniki, sistem svyazi i upravleniya 2015:29-32. (in Russian)].

19. Мавринская Т.В., Лошкарев А.В., Чуракова Е.Н. Обезличивание персональных данных и технологии «больших данных» (Big Data). *Интерактивная наука* 2017;16(6):78-80. [Mavrinskaya T.V., LoshkarYov A.V., Churakova E.N. Obezlichivanie personalnyih dannyih i tehnologii «bolshih dannyih» (Big Data). *Interaktivnaya nauka = Interactive science* 2017;16(6):78-80. (in Russian)].

20. Santos J. The myth of anonymization: has big data killed anonymity? Kantar Health 2015. URL: http://www.kantarhealth.com/docs/white-papers/the-myth-of-anonymization-has-big-data-killed-anonymity-.pdf (date of the application: 16.08.2021).

21. Mismatch S. Организация защиты информации в телемедицинских консультативно-диагностических системах. [Электронный ресурс]. https://pandia.ru/text/78/115/99552.php. [Mismatch S. Organizatsiya zaschityi informatsii v telemeditsinskih konsultativno-diagnosticheskih sistemah. [Elektronnyiy resurs]. https://pandia.ru/text/78/115/99552.php. (in Russian)].

22. Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности». [Электронный ресурс]. URL: https://rg.ru/2014/09/17/zashita-dok.html. [Prikaz Federalnoy sluzhbyi bezopasnosti Rossiyskoy Federatsii ot 10 iyulya 2014 g. # 378 g. «Ob utverzhdenii Sostava i soderzhaniya organizatsionnyih i tehnicheskih mer po obespecheniyu bezopasnosti personalnyih dannyih pri ih obrabotke v informatsionnyih sistemah personalnyih dannyih s ispolzovaniem sredstv kriptograficheskoy zaschityi informatsii, neobhodimyih dlya vyipolneniya ustanovlennyih Pravitelstvom Rossiyskoy Federatsii trebovaniy k zaschite personalnyih dannyih dlya kazhdogo iz urovney zaschischennosti». [Elektronnyiy resurs]. URL: https://rg.ru/2014/09/17/zashita-dok.html. (in Russian)].

23. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (Решение председателя Гостехкомиссии России от 30 марта 1992 г.). [Электронный ресурс]. https://fstec.ru/index?id=384:rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g. [Avtomatizirovannyie sistemyi. Zaschita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannyih sistem i trebovaniya po zaschite informatsii (Reshenie predsedatelya Gostehkomissii Rossii ot 30 marta 1992 g.). [Elektronnyiy resurs]. https://fstec.ru/index?id=384:rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g. (in Russian)].

24. Государственный реестр сертифицированных средств защиты информации. [Электронный ресурс]. https://fstec.ru/tekhnicheskaya-zaschita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591. [Gosudarstvennyiy reestr sertifitsirovannyih sredstv zaschityi informatsii. [Elektronnyiy resurs]. https://fstec.ru/tekhnicheskaya-zaschita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591. (in Russian)].

25. Чередниченко А. Системы защиты персональных данных. *Т-Comm: Телекоммуникации и транспорт* 2009;3(6):22-24. [Cherednichenko A. Sistemyi zaschityi personalnyih dannyih. *T-Comm: Telekommunikatsii i transport = T-Comm* 2009;3(6):22-24. (in Russian)].

26. Hongyang Yan, Jin Li, Xuan Li, Gansen Zhao, Sun-Young Lee, and Jian Shen. Secure access control of e-Health system with attribute-based encryption. *Intelligent Automation & Soft Computing* 2006;22(3):345–52.

27. Daly A. The law and ethics of «self-quantified» health information: an Australian perspective. *International Data Privacy Law* 2015;5(2):154.

28. Рыжов Р.С. Электронная медицина, как накопитель конфиденциальной информации о гражданах и проблемы его правового обеспечения. *Пробелы в российском законодательстве* 2012;(2):277-280. [Ryizhov R.S. Elektronnaya meditsina, kak nakopitel konfidentsialnoy informatsii o grazhdanah i problemyi ego pravovogo obespecheniya. *Probelyi v rossiyskom zakonodatelstve = Gaps in Russian Legislation* 2012;(2):277-280. (in Russian)].

29. Сергиенко Л.А. Защита персональных данных и Интернет. *Информационное общество* 2000;(4):44-45. [Sergienko L.A. Zaschita personalnyih dannyih i Internet. *Informatsionnoe obschestvo = Information Society* 2000;(4):44-45. (in Russian)].

30. Журавлев М.С. Защита персональных данных в телемедицине. *Право. Журнал высшей школы экономики* 2016;(3):72-84. [ZhuravlYov M.S. Zaschita personalnyih dannyih v telemeditsine. *Pravo. Zhurnal vyisshey shkolyi ekonomiki = Law. Journal of the Higher School of Economics* 2016;(3):72-84. (in Russian)].

ЛИТЕРАТУРА

31. Наумов В.Б., Савельев Д.А. Правовые аспекты телемедицины. СПб.: Анатолия, 2002; 107 с. [Naumov V.B., Savelev D.A. Pravovyie aspektyi telemeditsinyi. SPb.: Anatoliya, 2002; 107 c. (in Russian)].
32. Богдановская И.Ю. Правовое регулирование телемедицины: опыт США. *Врач и информационные технологии* 2007;(3):64–68. [Bogdanovskaya I.Yu. Pravovoe regulirovanie telemeditsinyi: opyit SShA. *Vrach i informatsionnyie tehnologii = Physicians and IT* 2007;(3):64–68. (in Russian)].
33. Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации». [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/32206/page/1. [Federalnyiy zakon ot 29.11.2010 # 326-FZ «Ob obyazatelnom meditsinskom strahovanii v Rossiyskoy Federatsii». [Elektronnyiy resurs]. URL: http://www.kremlin.ru/acts/bank/32206/page/1. (in Russian)].
34. Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data). *Право. Журнал Высшей школы экономики* 2015;(1):43–67. [Savelev A.I. Problemyi primeneniya zakonodatelstva o personalnyih dannyih v epohu «Bolshih dannyih» (Big Data). *Pravo. Zhurnal Vyisshey shkolyi ekonomiki = Law. Journal of the Higher School of Economics* 2015;(1):43–67. (in Russian)].
35. Mantovani E, Quinn P. mHealth and data protection — the letter and the spirit of consent legal requirements. *International Review of Law, Computers & Technology* 2014;28(2):222.
36. Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323- ФЗ [Электронный ресурс]. URL: http://www.consultant. ru/document/cons_doc_LAW_121895/ (Дата обращения: 22.11.2020). [Federalnyiy zakon «Ob osnovah ohranyi zdorovya grazhdan v Rossiyskoy Federatsii» ot 21.11.2011 # 323- FZ [Elektronnyiy resurs]. URL: http://www.consultant. ru/document/cons_doc_LAW_121895/ (Data obrascheniya: 22.11.2020). (in Russian)].
37. Шадеркин И.А., Зеленский М.М., Шадеркина В.А. Телемедицина: мнение урологов. *Журнал телемедицины и электронного здравоохранения* 2020;6(1):36–44. [Shaderkin I.A., Zelenskiy M.M., Shaderkina V.A. Telemeditsina: mnenie urologov. *Zhurnal telemeditsinyi i elektronnogo zdravoohraneniya = Journal of Telemedicine and E-Health* 2020;6(1):36–44. (in Russian)].
38. Федеральный закон от 8 июня 2020 г. № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации». [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/74132857/ (дата обращения: 22.11.2020). [Federalnyiy zakon ot 8 iyunya 2020 g. # 168-FZ «O edinom federalnom informatsionnom registre, soderzhaschem svedeniya o naselenii Rossiyskoy Federatsii». [Elektronnyiy resurs]. URL: https://www.garant.ru/products/ipo/ prime/doc/74132857/ (data obrascheniya: 22.11.2020). (in Russian)].
39. Приказ Минздрава России от 30.11.2017 № 965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий». [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201801100021?index=1&rangeSize=1. [Prikaz Minzdrava Rossii ot 30.11.2017 # 965n «Ob utverzhdenii poryadka organizatsii i okazaniya meditsinskoy pomoschi s primeneniem telemeditsinskih tehnologiy». [Elektronnyiy resurs]. URL: http://publication.pravo.gov.ru/Document/View/0001201801100021?index=1&rangeSize=1. (in Russian)].
40. Письмо Минздрава России от 09.04.2018 № 18-2/0579 «О порядке организации и оказания медицинской помощи с применением телемедицинских технологий». [Электронный ресурс]. URL: https://rulaws.ru/acts/Pismo-Minzdrava-Rossii-ot-09.04.2018-N-18-2_0579/. [Pismo Minzdrava Rossii ot 09.04.2018 # 18-2/0579 «O poryadke organizatsii i okazaniya meditsinskoy pomoschi s primeneniem telemeditsinskih tehnologiy». [Elektronnyiy resurs]. URL: https://rulaws.ru/acts/Pismo-Minzdrava-Rossii-ot-09.04.2018-N-18-2_0579/. (in Russian)].
41. Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации». [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/45796. [Federalnyiy zakon ot 31.07.2020 # 258-FZ «Ob eksperimentalnyih pravovyih rezhimah v sfere tsifrovyih innovatsiy v Rossiyskoy Federatsii». [Elektronnyiy resurs]. URL: http://www.kremlin.ru/acts/bank/45796. (in Russian)].
42. Федеральный закон от 30 декабря 2020 г. № 159-ФЗ «О внесении изменений в закон «О персональных данных». [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202012300044. [Federalnyiy zakon ot 30 dekabrya 2020 g. # 159-FZ «O vnesenii izmeneniy v zakon «O personalnyih dannyih». [Elektronnyiy resurs]. URL: http://publication.pravo.gov.ru/Document/View/0001202012300044. (in Russian)].
43. Законопроект № 174692-7 «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья». [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/174692-7 (Дата обращения: 22.08.2021). [Zakonoproekt # 174692-7 «O vnesenii izmeneniy v otdelnyie zakonodatelnyie aktyi Rossiyskoy Federatsii po voprosam primeneniya informatsionnyih tehnologiy v sfere ohranyi zdorovya». [Elektronnyiy resurs]. URL: https://sozd.duma.gov.ru/bill/174692-7 (Data obrascheniya: 22.08.2021). (in Russian)].

Сведения об авторах:

Монаков Д.М. – к.м.н., врач урологического отделения ГКБ им. С. П. Боткина; Москва, Россия; ассистент кафедры урологии и оперативной нефрологии с курсом онкоурологии ФНМО МИ РУДН; gvkg-monakov@mail.ru

Шадеркина В.А. – научный редактор урологического информационного портала UroWeb.ru; Москва, Россия; РИНЦ Author ID 880571

Рева С.А. – к.м.н., заведующий 6 онкологическим отделением (андрологии и онкоурологии), НИЦ Урологии, ФГБОУ ВО «Первыи Санкт-Петербургскии государственныи медицинскии университет им. акад. И.П. Павлова», научныи сотрудник ФГБУ «НМИЦ онкологии им. Н.Н. Петрова»; Санкт-Петербург, Россия; РИНЦ AuthorID 801853

Грицкевич А.А. – д.м.н., профессор кафедры урологии с курсами онкологии, радиологии и андрологии ФНМО МИ РУДН, заведующий отделением урологии ФГБУ «Национальный медицинский исследовательский центр хирургии им. А.В. Вишневского» Минздрава России; Москва, Россия; РИНЦ AuthorID 816947

Вклад авторов:
Монаков Д.М. – литературный обзор, написание текста статьи, 30%
Шадеркина В.А. – дизайн обзора, написание текста статьи, 30%
Рева С.А. – литературный обзор, 20%
Грицкевич А.А. – определение научного интереса, дизайн публикации, 20%

Конфликт интересов: Авторы заявляют об отсутствии конфликта интересов.

Финансирование: Исследование проведено без спонсорской поддержки.

Статья поступила: 14.07.21
Результаты рецензирования: 22.07.21
Принята к публикации: 27.09.21

Information about authors:

Monakov D.M. – MD, PhD, urologist of the consultative department of the CCH im. S.P. Botkin; Moscow, Russia; assistant of the department of urology and operative nephrology with the course of oncourology of the Peoples' friendship university of Russia; gvkg-monakov@mail.ru; https://orcid.org/0000-0002-9676-1802

Shaderkina V.A. – MD, scientific editor of the urological information portal UroWeb.ru; Moscow, Russia; https://orcid.org/0000-0002-8940-4129

Reva S.A. – MD, PhD, head of the Department of oncology No6 (of andrology and oncourology), Research Center of Urology, Pavlov First St. Petersburg State, Medical University, St. Peters- burg, Russia; researcher, N.N. Petrov Research Institute of Oncology; Saint-Petersburg, Russia; https://orcid.org/0000-0001-5183-5153

Gritskevich A.A. – MD, PhD, Professor of the Department of Urology with the course of oncology, radiology and andrology of Peoples' friendship university of Russia, the head of the Urology department of A.V. Vishnevsky National Medical Research Center of Surgery; Moscow, Russia; https://orcid.org/0000-0002-5160-925X

Authors Contribution:
Monakov D.M. – literary review, writing the text of the article, 30%
Shaderkina V.A. – design of the review, writing the text of the article, 30%
Reva S.A. – literature review, 20%
Gritskevich A.A. – definition of scientific interest, publication design, 20%

Conflict of interest. The authors declare no conflict of interest.

Financing. The study was performed without external funding.

Received: 14.07.21
Review results: 22.07.21
Accepted for publication: 27.09.21