УДК 349

Правовой режим информационных ресурсов медицинских информационных систем

Р. В. Амелин, Л. В. Бессонов

Амелин Роман Влидимирович, кандидат юридических наук, доцент кафедры конституционного и муниципального права, Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, ame-roman@yandex.ru

Бессонов Леонид Валентинович, кандидат физико-математических наук, ведущий научный сотрудник лаборатории «Системы поддержки принятия врачебных решений», Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, lexx.besson@gmail.com

Введение. Совокупность сведений, хранящихся в медицинских информационных системах (МИС), имеет важное значение и зачастую выступает как самостоятельный объект права. Особенностью медицинских информационных ресурсов является то, что в их составе, как правило, объединяется информация, подпадающая под действие различных специальных режимов, что порождает ряд специфических проблем. **Теоретический анализ.** Медицинская информация о здоровье пациента одновременно подпадает под две категории – врачебная тайна и персональные данные. Российское законодательство практически не предусматривает мер ответственности для оператора за утечку персональных данных, если формально приняты все требуемые законодательством меры по их защите. Между тем данные о состоянии здоровья нации представляют стратегическую ценность, а соответствующие информационные системы должны быть отнесены к объектам критической информационной инфраструктуры (КИИ). **Эмпирический анализ.** Базовым информационным ресурсом в сфере здравоохранения в настоящее время можно считать электронную медицинскую карту пациента, при этом в российском законодательстве отсутствует как ее признанное официальное определение, так и требования к ее содержанию, что приводит к сложностям интеграции медицинских данных и проблемам при определении ее юридической значимости. **Результаты.** Предложено распространить понятие объекта критической информационной инфраструктуры с информационных систем на информационные ресурсы, а также установить уголовную ответственность в случае причинения ущерба жизни людей вследствие атаки на медицинскую информационную систему (информационный ресурс), в отношении которой не была своевременно подана заявка о включении в реестр КИИ.

Ключевые слова: медицинские информационные ресурсы, врачебная тайна, критическая информационная инфраструктура, электронная медицинская карта.

DOI: https://doi.org/10.18500/1994-2540-2019-19-4-428-435

Введение

Совокупность сведений, хранящихся в медицинских информационных системах (МИС), имеет важное значение и зачастую выступает как самостоятельный объект права. Из отдельных сведений формируются такие структурные единицы, как документы (электронные документы) и базы данных. В ранее действовавшем Федеральном законе «Об информации, информатизации и защите информации» отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах) определялись как информационные ресурсы. В настоящее время термин «информационный ресурс» не имеет легальной дефиниции, но при этом используется во множестве законов и подзаконных нормативных актов [1, с. 103] (включая специальное Постановление Правительства РФ от 14.09.2012 № 928 «О базовых государственных информационных ресурсах»). Нами было предложено под информационным ресурсом понимать совокупность документированной информации, в отношении которой законом или иными нормативными правовыми актами установлен режим, включающий основания и порядок включения информации в состав информационного ресурса, порядок и условия ее предоставления и использования [2, с. 189]. Информационный ресурс существует независимо от информационной системы и имеет обособленный правовой режим, который оказывает влияние на правовой режим информационной системы. В частности, состав и содержание информационного ресурса, правовой статус поставщиков и пользователей информации следует считать элементами правового режима именно информационного ресурса. Значительное влияние на правовой режим информационного ресурса оказывает прямой правовой режим информации, входящей в его состав.

Особенностью медицинских информационных ресурсов является то, что в их составе, как правило, объединяется информация, подпадающая под действие различных специальных режимов. Значительная доля входящих в их состав сведений относится к категории медицинской тайны, которая одновременно является подвидом профессиональной тайны и тайны частной жизни. При этом сведения о здоровье пациентов, составляющие медицинскую тайну, одновременно отвечают признакам персональных данных. Статистическая медицинская информация

и ряд других обобщенных сведений относятся к информации гарантированного доступа и в обязательном порядке предоставляются заинтересованным лицам посредством медицинских информационных систем. Это порождает ряд специфических правовых проблем и сложностей юридического характера при формировании и использовании медицинских информационных ресурсов.

Теоретический анализ

Медицинская информация о здоровье пациента одновременно подпадает под две категории – врачебная тайна и персональные данные. Врачебная тайна регулируется ст. 13 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (далее – Закон об охране здоровья) [3]. Обязанность ее неразглашения накладывается на медицинский персонал. Специальной нормы, устанавливающей ответственность за разглашение врачебной тайны, в законодательстве нет, однако лицо может быть привлечено к административной ответственности по ст. 13.14 КоАП РФ (разглашение информации с ограниченным доступом) и ст. 137 УК РФ (нарушение неприкосновенности частной жизни). Гражданин вправе в досудебном порядке обратиться к медицинской организации с требованием о возмещении вреда, в том числе морального, или обратиться с исковым заявлением в суд. В зависимости от обстоятельств дела требования могут быть основаны в том числе на ст. 15, 150, 151, 1064, 1068, 1099, 1101 ГК РФ и законодательстве о защите прав потребителей и персональных данных [4]. Право пациента на врачебную тайну ограничивается на основаниях, предусмотренных ч. 4 ст. 13 (например, при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений), при этом в российском законодательстве, в отличие от законодательства некоторых зарубежных стран, отсутствует институт оповещения пациента о таком ограничении [5].

В случае, когда информация о здоровье пациента накапливается, хранится и обрабатывается в электронной форме, она подпадает под действие законодательства о персональных данных. Под персональными данными в соответствии со ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) понимается любая информация, относящаяся к физическому лицу, которое может быть прямо или косвенно определено и связано с этой информацией [6]. Информационные системы, в базах данных которых хранятся персональные данные, относятся к особой категории – информационные системы персональных данных (ИСПД), и на них накладываются дополнительные требования [7].

Следует отметить, что информация о состоянии здоровья относится к одной из специальных категорий (наряду со сведениями о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни), обработка которых не допускается в соответствии со ст. 10 Закона о персональных данных. При этом ч. 4 ст. 10 содержит исключение, которым охватывается подавляющее большинство ситуаций – если обработка осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну. Проблема заключается в том, что в мире современных информационных технологий накопленные данные довольно часто становятся доступны иным лицам. Речь идет об утечках и взломах информационных систем.

Российское законодательство предъявляет множество административных требований к процедурам обработки персональных данных, документационному обеспечению этих процедур – настолько, что можно говорить о чрезмерной зарегулированности и необоснованном бремени операторов персональных данных (особенно организаций малого бизнеса) по соблюдению всех регламентов. При этом реальная защищенность персональных данных значительно ниже, чем сведений, относящихся к другим видам тайн [8]. Возможно, это объясняется тем, что, в отличие от государственной или коммерческой тайны, обработка и защита персональных данных осуществляется не теми субъектами, которые заинтересованы в их сохранности. Российское законодательство практически не предусматривает мер ответственности для оператора за утечку персональных данных, если формально приняты все требуемые законодательством меры по их защите [9, с. 5].

Между тем, на наш взгляд, данные о состоянии здоровья нации представляют стратегическую ценность. Для нас очевидно, что бесконтрольное распространение таких данных в целом может представлять угрозу для интересов Российской Федерации. Кроме этого, хотя обеспечение конфиденциальности, целостности и доступности медицинских данных одного пациента в масштабах государства не представляет важности (пусть даже критически важно для самого

этого пациента), но из этих отдельных данных и складывается цифровой контур здравоохранения. С развитием интернета вещей, дистанционно управляемых медицинских приборов, ведением медицинской документации в электронном виде последствия несанкционированного доступа к электронным медицинским данным становятся все опаснее, поскольку данные могут быть не только похищены, но и изменены. В случае массового нарушения целостности персональных медицинских данных это может привести к катастрофе в национальном масштабе. Мы видим решение в том, чтобы отнести информационные системы, обрабатывающие медицинские информационные ресурсы, к критической информационной инфраструктуре (КИИ).

Отношения в области безопасности критической информационной инфраструктуры регулируются Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [10]. Следует отметить, что согласно п. 7 ст. 2 к объектам критической информационной инфраструктуры могут быть отнесены только информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. Мы видим в этом потенциальный пробел законодательства, поскольку вследствие усилившейся в последние годы тенденции к интеграции различных информационных систем и сервисов доступ к информационным ресурсам одной ИС, относящейся к объектам критической инфраструктуры, может быть получен средствами другой, которая не относится к указанной категории. С учетом того, что, как показано выше, правовой режим информационной системы во многом определяется правовым режимом ее информационных ресурсов, понятие объекта критической информационной инфраструктуры вполне целесообразно распространить и на информационные ресурсы.

Решение о включении сведений о значимом объекте критической информационной инфраструктуры в реестр принимается в течение 30 дней со дня получения Федеральной службой по техническому и экспортному контролю России (ФСТЭК) сведений от субъекта критической информационной инфраструктуры [11]. При этом к субъектам критической информационной инфраструктуры отнесены государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на правах собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в том числе в сфере здравоохранения. Однако, как справедливо отмечает Э. В. Горян, в ФЗ-187 и связанных подзаконных актах отсутствует положение по отнесению организации к субъектам КИИ: каким образом и на каких основаниях будет происходить такая процедура. В такой ситуации или организации должны проявить инициативу и самостоятельно провести идентификацию своих информационных сетей как КИИ с последующим категорированием объектов КИИ и уведомлением уполномоченного федерального органа, или уполномоченный федеральный орган должен издать соответствующее предписание в отношении определенных информационных сетей и организаций. Такая неопределенность замедляет идентификацию КИИ и, соответственно, эффективность обеспечения ее безопасности [12].

По нашему мнению, к категории объектов КИИ должны быть отнесены не все информационные системы в сфере здравоохранения (что на данном этапе только добавит непосильную административную нагрузку на медицинские организации), а те системы (а также информационные ресурсы), нарушение конфиденциальности, целостности или доступности которых создает угрозу причинения ущерба жизни и здоровью людей. Следует отметить, что Правила категорирования объектов КИИ РФ [13] включают такой показатель: системы, для которых он составляет от 1 до 50 пострадавших, относятся к III категории, а более 500 – к I категории. Следует законодательно предусмотреть административную ответственность за нарушение обязанности оператора (владельца) такого объекта подачи сведений для включения в реестр КИИ, а также уголовную ответственность в случае причинения ущерба жизни людей вследствие атаки на медицинскую информационную систему (информационный ресурс), в отношении которой не была своевременно подана заявка о включении в реестр КИИ.

Говоря о персональных данных в медицинской сфере, следует также отметить особенности процедуры их обезличивания. Согласно п. 9 ст. 3 Закона о персональных данных, обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту. Обезличенные персональные данные не являются информацией ограниченного доступа и могут использоваться в статистических или иных исследовательских целях (п. 9 ч. 1 ст. 6).

При обезличивании персональных данных в медицинской сфере имеется необходимость сохранения большого числа данных в связном виде. Для медицинских исследований, в частности, необходимо хранение полной истории болезни, которая может включать множество документов, относящихся к различным временным интервалам. Другими словами, хотя принадлежность персональных данных конкретному лицу может скрываться, важен тот факт, что некоторая совокупность персональных данных относится к одному и тому же лицу. Этот способ обезличивания называется *псевдонимизацией* (присвоение пациенту секретного «псевдонима»), и в отличие от *анонимизации* она обратима, т.е. при определенных условиях возможна обратная персонификация. Как отмечает М. С. Журавлев, в эпоху развития технологий анализа «больших данных» способность обезличивания становится весьма условной [14].

Как следствие, на наш взгляд, требуется нормативное закрепление специальных требований к обезличиванию медицинских персональных данных на основе присвоения псевдонима. Помимо достаточно очевидных правил (псевдоним не должен быть известен ни врачу, ни пациенту; псевдоним не должен указываться на первичных и учетных документах; в качестве псевдонима не должны использоваться иные персональные данные, такие как СНИЛС, ИНН и т.д.), должны быть установлены дополнительные обязанности субъектов, обрабатывающих псевдонимизированные медицинские данные, т.е. свободный доступ к ним должен быть исключен.

Эмпирический анализ

К наиболее ценным информационным ресурсам в сфере здравоохранения относятся:

– базы данных застрахованного населения, включая данные о льготных категориях граждан;

– базы персонифицированных медицинских данных о больных социально значимыми болезнями (регистры онкологических больных, больных туберкулезом, диабетом, ВИЧ-инфицированных больных и др.);

– медико-статистические базы персонифицированных данных медицинских услуг, включая услуги амбулаторно-поликлинической, стационарной, скорой и неотложной медицинской помощи, стоматологической помощи;

– базы данных по кадровому составу и материально-техническому оснащению ЛПУ;

– базы финансово-экономической информации;

– базы фармако-экономических данных, регистры лекарственных средств;

– базы нормативно-справочной информации и др. [15].

Статья 50 Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» предусматривает в качестве одной из целей модернизации здравоохранения ведение медицинских карт пациентов в электронном виде [16]. Рекомендация ведения электронной медицинской карты пациента и электронной истории болезни содержится в Распоряжении Правительства РФ от 29.12.2014 № 2769-р «Об утверждении Концепции региональной информатизации». *Электронная медицинская карта* (ЭМК) пациента – это совокупность электронных персональных медицинских записей (ЭПМЗ), относящихся к одному пациенту, собираемых, хранящихся и используемых в рамках одной медицинской организации [17]. В свою очередь, ЭПМЗ – любая медицинская запись, сохраненная на электронном носителе (ГОСТ Р 52636-2006). ЭПМЗ привязана к конкретному электронному хранилищу, характеризуется моментом размещения в этом хранилище.

Как отмечает М. Ю. Старчиков, повсеместное внедрение ЭМК объединит в единую сеть данные, разрозненно хранящиеся во множестве учреждений здравоохранения, позволяя срочно получать информацию, необходимую для неотложного медицинского вмешательства; позволит пациентам без помех и в удобное для них время реализовывать право на получение своей медицинской информации; поможет избежать споров о достоверности информации, касающейся обстоятельств и сути оказанной медицинской помощи, обеспечить полноту сбора подобных данных [18].

Следует отметить, что пациент либо его законный представитель имеет право непосредственно знакомиться с медицинской документацией и получать на основании такой документации консультации у других специалистов (ч. 4 ст. 22 Закона об охране здоровья). Также на основании запроса, направленного в том числе в электронной форме, пациент или его законный представитель имеют право получать отражающие состояние здоровья пациента медицинские документы (их копии) и выписки из них, в том числе в форме электронных документов (ч. 5 ст. 22 Закона об охране здоровья; п. 13, 16 Положения о ЕГИСЗ) [19].

С технической точки зрения электронная медицинская карта пациента – составной сборный медицинский документ, содержащий множество отдельных записей и документов, заверенных электронной подписью медицинского работника – автора записи. В зависимости от содержания в составе ЭМК можно выделить следующие разделы (блоки) данных: а) содержащие

персональные, социально-демографические и административные данные пациента; б) данные о врачебных назначениях и их выполнении; в) документированная клиническая информация, на основе которой осуществляется принятие врачебных решений [20].

Несмотря на отдельные общие рекомендации по ведению ЭМК, в частности, содержащиеся в методических рекомендациях по обеспечению функциональных возможностей МИС медицинских организаций, в российском законодательстве отсутствует как признанное официальное определение электронной медицинской карты, так и требования к ее содержанию. В настоящее время различные регионы, а в ряде случаев – различные медицинские организации в рамках одного региона по-разному решают эти вопросы, что приводит к сложностям интеграции медицинских данных. Н. Н. Штыкова отмечает опасность, которую представляет использование различных информационных (электронных) шаблонов для описания истории болезни, постановки диагноза и выбора вида лечения [21]. Очень многое зависит от культуры ведения информационных ресурсов в медицинских учреждениях (где в поле «ФИО» медицинской электронной карты вполне может встречаться запись «От главврача», а данные о пациенте могут вводиться несколько раз с различными идентификаторами).

Нельзя не согласиться с тем, что электронные медицинские документы повышают доступность медицинской информации, на основе анализа которой принимаются управленческие решения, а также при возникновении претензий со стороны пациентов и их представителей в случае ненадлежащего оказания медицинской помощи [22, с. 5]. Однако наиболее значимый эффект для развития «цифрового здравоохранения» будет, на наш взгляд, достигнут только после значительной унификации ЭМК. Унификация ЭМК позволит не только создавать в автоматизированном режиме обезличенные наборы «открытых данных» для построения агрегирующих сервисов, но и создать единый развитый и удобный механизм оказания в электронном виде государственной услуги по доступу к своим медицинским данным. В то же время следует согласиться с М. Ю. Старчиковым в том, что для полноценного внедрения ЭМК необходимо решить ряд проблемных вопросов, в том числе проблему правовой неопределенности электронного документооборота в медицинских организациях – особенно «смешанного» электронного документооборота, при котором карты пациентов ведутся как в бумажном, так и в электронном виде [23, с. 41]. Автор обращает внимание на неопределенность юридической значимости электронных медицинских карт при рассмотрении судами дел о некачественном оказании медицинских услуг. В то же время можно констатировать появление судебной практики, связанной со спорами о ведении медицинской документации в электронном виде [24, 25].

Результаты

Подводя итог вышесказанному, можно сделать ряд выводов теоретического и практического характера.

Медицинские информационные ресурсы представляют собой важный самостоятельный объект правового регулирования, правовой режим которого оказывает определяющее влияние на правовой режим медицинских информационных систем.

При отнесении медицинских информационных систем к объектам критической информационной инфраструктуры следует исходить из того, что не любая информационная система в сфере здравоохранения должна быть отнесена к КИИ (так как на данном этапе это только добавит непосильную административную нагрузку на медицинские организации), а те системы, нарушение конфиденциальности, целостности или доступности которых создает угрозу причинения ущерба жизни и здоровью людей. Следует законодательно предусмотреть административную ответственность за нарушение обязанности оператора (владельца) такого объекта по передаче сведений для включения в реестр КИИ, а также уголовную ответственность в случае причинения ущерба жизни людей вследствие атаки на медицинскую информационную систему (информационный ресурс), в отношении которой не была своевременно подана заявка о включении в реестр КИИ.

Вследствие усилившейся в последние годы тенденции к интеграции различных информационных систем и сервисов доступ к информационным ресурсам одной информационной системы, относящейся к объектам критической инфраструктуры, может быть получен средствами другой, которая не относится к указанной категории. Эта проблема может быть частично решена, если распространить понятие объекта критической информационной инфраструктуры с информационных систем на информационные ресурсы.

Благодарности

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 17-03-00082-ОГН).

Список литературы

1. *Ковалева Н. Н.* Административно-правовое регулирование использования информационных технологий в государственном управлении : дис. … д-ра юрид. наук. Саратов, 2014. 336 с.
2. *Амелин Р. В.* Государственные и муниципальные информационные системы в российском информационном праве : теоретико-правовой анализ. М. : ГроссМедиа, 2018. 324 с.
3. Об основах охраны здоровья граждан в Российской Федерации : федер. закон от 21.11.2011 № 323-ФЗ // Собр. законодательства Рос. Федерации. 2011. № 48, ст. 6724.
4. *Старчиков М. Ю.* Административная ответственность медицинских работников : основания наступления, комментарии юриста и судебная практика. Доступ из справ.-правовой системы «КонсультантПлюс».
5. *Павлов А. В.* Правовое регулирование общественных отношений по поводу врачебной тайны в Королевстве Дания и в Российской Федерации : сравнительный анализ // Журнал зарубежного законодательства и сравнительного правоведения. 2017. № 4. С. 74–80.
6. О персональных данных : федер. закон от 27.07.2006 № 152-ФЗ // Собр. законодательства Рос. Федерации. 2006. № 31 (ч. 1), ст. 3451.
7. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства РФ от 01.11.2012 № 1119 // Собр. законодательства Рос. Федерации. 2012. № 45, ст. 6257.
8. *Амелин Р. В.* О правовых принципах разработки государственных АИС, обрабатывающих персональные данные // Информационное право. 2009. № 2. С. 32–35.
9. *Али М.* Персональные данные : обязанности и ответственность оператора // ЭЖ-Юрист. 2017. № 12. С. 5–8.
10. О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон от 26.07.2017 № 187-ФЗ // Собр. законодательства Рос. Федерации. 2017. № 31 (ч. 1), ст. 4736.
11. Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации : приказ ФСТЭК России от 06.12.2017 № 227. Доступ из справ.-правовой системы «КонсультантПлюс».
12. *Горян Э. В.* Институциональные механизмы обеспечения безопасности критической информационной инфраструктуры Российской Федерации и Сингапура : сравнительно-правовой аспект // Административное и муниципальное право. 2018. № 9. С. 49–60.
13. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений : постановление Правительства РФ от 08.02.2018 № 127 // Собр. законодательства Рос. Федерации. 2018. № 8, ст. 1204.
14. *Журавлев М. С.* Правовое обеспечение электронного документооборота в телемедицине // Информационное право. 2017. № 4. С. 10–15.
15. *Мартыненко В. Ф., Вялкова Г. М., Полесский В. А., Беляев Е. Н., Гройсман В. А., Серегина И. Ф.* Информационные ресурсы здравоохранения // ГлавВрач. 2007. № 4. С. 88–92.
16. Об обязательном медицинском страховании в Российской Федерации : федер. закон от 29.11.2010 № 326-ФЗ // Собр. законодательства Рос. Федерации. 2010. № 49, ст. 6422.
17. Основные разделы электронной медицинской карты : утв. Минздравом России 11.11.2013 № 18-1/1010. Доступ из справ.-правовой системы «КонсультантПлюс».
18. *Старчиков М. Ю.* Электронная медицинская карта в отечественном здравоохранении : юридическая регламентация и судебная практика.Доступ из справ.-правовой системы «КонсультантПлюс».
19. Имеет ли пациент право на получение информации о состоянии своего здоровья? // Азбука права : электрон. журн. 2019. Доступ из справ.-правовой системы «КонсультантПлюс».
20. *Столбов А. П.* О критериях оценки уровня выполнения функции «ведение электронной медицинской карты пациента» // Врач и информационные технологии. 2017. № 1. С. 24–39.
21. *Штыкова Н. Н.* Сущность и проблемы реализации электронной медицины (на примере Владимирской области) // Медицинское право. 2014. № 5. С. 22–27.
22. *Китанина К. Ю., Рублевская И. В., Честнова Т. В., Хромушин В. А.* Сборник медицинских документов (часть 1) : учеб. пособие. Тула : Изд-во ТулГУ, 2013. 451 с.
23. *Старчиков М. Ю.* Юридически значимые медицинские документы : нормативные положения, типовые формы и судебная практика (справочное пособие с ситуационными задачами и ответами на них). М. : Инфотропик Медиа, 2018. 314 с.
24. Решение Арбитражного суда г. Москвы от 29.10.2010 по делу № А40-76535/10-151-644 // Федеральные арбитражные суды Российской Федерации. URL: http://kad.arbitr.ru (дата обращения: 11.06.2019).
25. Постановление Девятого арбитражного суда от 26.01.2011 № 09АП-33523/2010-ГК по делу № А40-76535/10-151-644 // Федеральные арбитражные суды Российской Федерации. URL: http://kad.arbitr.ru (дата обращения: 11.06.2019).

Образец для цитирования:

Амелин Р. В., Бессонов Л. В. Правовой режим информационных ресурсов медицинских информационных систем // Изв. Сарат. ун-та. Нов. сер. Сер. Экономика. Управление. Право. 2019. Т. 19, вып. 4. С. 428–435. DOI: https://doi.org/10.18500/1994-2540-2019-19-4-428-435

The Legal Regime of Information Resources of Medical Information Systems

R. V. Amelin, L. V. Bessonov

Roman V. Amelin, https://orcid.org/0000-0002-7054-5757, Saratov State University, 83 Astrakhanskaya St., Saratov 410012, Russia, ame-roman@yandex.ru

Leonid V. Bessonov, https://orcid.org/0000-0002-5636-1644, Saratov State University, 83 Astrakhanskaya St., Saratov 410012, Russia, lexx.besson@gmail.com

Introduction. The collection of information stored in medical information systems is important and often acts as an independent object of law. A specific feature of medical information resources is that they usually include information that falls under the action of various special regimes, which gives rise to a number of specific legal problems. **Theoretical analysis.** Medical information about a patient's health at the same time falls into two categories – medical confidentiality and personal data. Russian legislation practically does not provide the operator with the measures of responsibility for the leakage of personal data if all measures stipulated by the legislation for their protection have been formally taken. Meanwhile, the data on the state of health of a nation are of strategic value, and the corresponding information systems should be referred to as the objects of critical information infrastructure (CII). **Empirical analysis.** At present, the patient's electronic medical record is a basic information resource in the healthcare sector, while Russian legislation lacks both its recognized official definition and its content requirements, which leads to difficulties in integrating medical data and problems in determining its legal significance. **Results.** It was proposed to extend the concept of a critical information infrastructure object from information systems to information resources, and to establish criminal liability in case of damage to people's lives due to an attack on a medical information system (information resource), for which the application for inclusion in CII registry was not filed in a timely manner.

Keywords: medical information resources, medical secrecy, critical information infrastructure, electronic medical record.

Acknowledgements: *This work was supported by the Russian Foundation for Basic Research (project No. 17-03-00082-ОГН).*

References

1. Kovaleva N. N. *Administrativno-pravovoe regulirovanie ispol'zovaniya informatsionnykh tekhnologiy v gosudarstvennom upravlenii* [Administrative and legal regulation of the use of information technology in public administration]. Diss. Dr. Sci. (Jur.). Saratov, 2014. 336 p. (in Russian).
2. Amelin R. V. *Gosudarstvennye i munitsipal'nye informatsionnye sistemy v rossiiskom informatsionnom prave: teoretiko-pravovoi analiz* [State and Municipal Information Systems in Russian Information Law: Theoretical and Legal Analysis]. Moscow, GrossMedia Publ., 2018. 324 p. (in Russian).
3. On the basis of public health protection in the Russian Federation. Federal law of 21.11.2011 no. 323-FZ. *Sobranie zakonodatel'stva RF* [Collection of Laws of the Russian Federation], 2011, no. 48, art. 6724 (in Russian).
4. Starchikov M. Yu. *Administrativnaia otvetstvennost' meditsinskikh rabotnikov: osnovaniya nastupleniya, kommentarii jurista i sudebnaia praktika* (Administrative responsibility of medical professionals: grounds of evidence, legal commentary and court practice). *ATP «Consultant»* [electronic resource] (in Russian).
5. Pavlov A. V. Legal regulation of public relations regarding medical secrecy in the Kingdom of Denmark and in the Russian Federation: a comparative analysis. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* [Journal of Foreign Law and Comparative Law], 2017, no. 4, pp. 74–80 (in Russian).
6. On personal data. Federal law of 27.07.2006 no. 152-FZ. *Sobranie zakonodatel'stva RF* [Collection of Laws of the Russian Federation], 2006, no. 31 (pt. 1), art. 3451 (in Russian).
7. On approval of requirements for the protection of personal data during their processing in personal data information systems. Decree of the Government of the Russian Federation of 01.11.2012 no. 1119. *Sobranie zakonodatel'stva RF* [Collection of Laws of the Russian Federation], 2012, no. 45, art. 6257(in Russian).
8. Amelin R. V. On the legal principles for the development of public AIS processing personal data. *Informatsionnoe pravo* [Information Law], 2009, no. 2, pp. 32–35 (in Russian).
9. Ali M. Personal data: duties and responsibilities of the operator. E*Zh-Jurist* [Electronic Journal Lawyer], 2017, no. 12, pp. 5–8 (in Russian).
10. On security of critical information infrastructure of the Russian Federation. Federal law of 26.07.2017 no. 187-FZ. *Sobranie zakonodatel'stva RF* [Collection of Laws of the Russian Federation], 2017, no. 31 (pt. 1), art. 4736 (in Russian).
11. On approval of the procedure for maintaining the register of significant objects of the critical information infrastructure of the Russian Federation. Order of the Federal Service for Technical and Export Control of Russia of 06.12.2017 no. 227. *ATP «Consultant»* [electronic resource] (in Russian).
12. Gorjan E. V. Institutional mechanisms to ensure the security of the critical information infrastructure of the Russian Federation and Singapore: a comparative legal aspect. *Administrativnoe i munitsipal'noe pravo* [Administrative and municipal law], 2018, no. 9, pp. 49–60 (in Russian).
13. On approval of the Rules for the categorization of objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of the criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values. Decree of the Government of the Russian Federation of 08.02.2018 no. 127. *Sobranie zakonodatel'stva RF* [Collection of Laws of the Russian Federation], 2018, no. 8, art. 1204 (in Russian).

14. Zhuravlev M. S. Legal support of electronic document circulation in telemedicine. *Informatsionnoe pravo* [Information Law], 2017, no. 4, pp.10–15 (in Russian).
15. Martynenko V. F., Vyalkova G. M., Polessky V. A., Belyaev E. N., Groysman V. A., Seregina I. F. Health Information Resources. *GlavVrach* [Chief Physician], 2007, no. 4, pp. 88–92 (in Russian).
16. On compulsory health insurance in the Russian Federation. Federal law of 29.11.2010 no. 326-FZ. *Sobranie zakonodatel'stva RF* [Collection of Laws of the Russian Federation], 2010, no. 49, art. 6422 (in Russian).
17. The main sections of the electronic medical card. Approved by Ministry of Health of Russia 11.11.2013 no. 18-1/1010. *ATP «Consultant»* [electronic resource] (in Russian).
18. Starchikov M. Yu. *Elektronnaia meditsinskaia karta v otechestvennom zdravookhranenii: juridicheskaia reglamentatsiya i sudebnaia praktika* (Electronic medical record in domestic health care: legal regulation and judicial practice). *ATP «Consultant»* [electronic resource] (in Russian).
19. Does the patient have the right to receive information about his state of health. *Azbuka prava: elektronnyi zhurnal* [ABC of law: electron. journal], 2019. *ATP «Consultant»* [electronic resource] (in Russian).
20. Stolbov A. P. On the criteria for assessing the level of implementation of the function "keeping an electronic medical card of the patient". *Vrach i informatsionnye tekhnologii* [Physicians and Information Technology], 2017, no. 1, pp. 24–39 (in Russian).
21. Shtykova N. N. Essence and problems of the implementation of e-medicine (on the example of the Vladimir region). *Meditsinskoe pravo* [Medical Law], 2014, no. 5, pp. 22–27 (in Russian).
22. Kitanina K. Yu., Rublevskaja I. V., Chestnova T. V., Hromushin V. A. *Sbornik meditsinskikh dokumentov (chast' 1)* [Collection of medical documents (Part 1). Tutorial]. Tula, Izdatel'stvo TulGU, 2013. 451 p. (in Russian).
23. Starchikov M. Yu. *Juridicheski znachimye meditsinskie dokumenty: normativnye polozheniya, tipovye formy i sudebnaia praktika (spravochnoe posobie s situatsionnymi zadachami i otvetami na nikh)* [Legally relevant medical documents: regulations, standard forms and court practice (reference book with situational tasks and answers to them)]. Moscow, Infotropik Media Publ., 2018. 314 p. (in Russian).
24. The decision of the Arbitration Court of Moscow, 29.10.2010 case no. A40-76535/10-151-644. *Federal'nye arbitrazhnye sudy Rossiiskoi Federatsii* (Federal Arbitration Courts of the Russian Federation). Available at: http://kad.arbitr.ru (accessed 11 June 2019) (in Russian).
25. Resolution of the Ninth Arbitration Court, 26.01.2011 no. 09AP-33523/2010-GK, case no. A40-76535/10-151-644. *Federal'nye arbitrazhnye sudy Rossiiskoi Federatsii* (Federal Arbitration Courts of the Russian Federation). Available at: http://kad.arbitr.ru (accessed 11 June 2019) (in Russian).

Cite this article as:

Amelin R. V., Bessonov L. V. The Legal Regime of Information Resources of Medical Information Systems. *Izv. Saratov Univ. (N. S.), Ser. Economics. Management. Law,* 2019, vol. 19, iss. 4, pp. 428–435 (in Russian). DOI: https://doi.org/10.18500/1994-2540-2019-19-4-428-435