УДК [004:614.253]:34.01 (4-672 ЕС)

ПРАВА ЧЕЛОВЕКА В АСПЕКТЕ ВЗАИМООТНОШЕНИЙ ВРАЧА И ПАЦИЕНТА В ЭРУ ЭЛЕКТРОННОГО ЗДРАВООХРАНЕНИЯ. ЧАСТЬ 1. ЕВРОПЕЙСКАЯ ПРАКТИКА ПРАВОВОГО РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ, СВЯЗАННЫХ С ОБРАЩЕНИЕМ СПЕЦИАЛЬНЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Н.Е.Хейфец, Е.Н.Хейфец

Республиканский научно-практический центр медицинских технологий, информатизации, управления и экономики здравоохранения (РНПЦ МТ), ул. П.Бровки, 7а, 220013, г. Минск, Республика Беларусь

Определена направленность правового механизма обеспечения прав пациента при внедрении электронного здравоохранения (ЭЗ). Изучены основные международные правовые акты о защите физических лиц при автоматизированной обработке специальных персональных данных, связанных со здоровьем (ДСЗ), и о свободном обращении таких данных. Сложившаяся практика правового регулирования вопросов обеспечения прав человека при оказании услуг ЭЗ в мире (право на выбор услуг, обязательное информированное согласие на услугу, право на отказ от оказания услуги, право собственного доступа и контроля доступа иных лиц (в том числе, медицинских работников) к персональной информации в системе ЭЗ, соблюдение врачебной тайны при свободном обращении ДСЗ и т.д.) изучена с целью разработки предложений по недопущению нарушения этих прав при формировании нормативно-правовой базы ЭЗ в Республике Беларусь.

Ключевые слова: взаимоотношения врача и пациента; электронное здравоохранение; специальные персональные данные, связанные со здоровьем; права человека; право на неприкосновенность личной жизни; врачебная тайна; правовое регулирование.

Введение. Стремительное развитие информационных технологий и средств коммуникации в последние десятилетия создает благоприятные предпосылки для информатизации процессов в здравоохранении. Оцифровка данных, в том числе, специальных персональных данных, связанных со здоровьем (ДСЗ), внедрение в повседневную практику все большего числа электронных сервисов и услуг, что позволяет уже на данном этапе рассматривать процесс оказания медицинской помощи в качестве основного компонента системы электронного здравоохранения (ЭЗ), понимаемого как совокупность информационно-коммуникационных технологий (ИКТ), направленных на совершенствование потока ДСЗ с целью обеспечения доступности и качества предоставления медицинских услуг и управления системой здравоохранения [1], обеспечивают существенные и явно наблюдаемые преимущества систем ЭЗ именно в указанных целевых областях. Перспективы реализации этих преимуществ, и ЭЗ в целом, связаны с тем, чтобы бесконечное накопление данных в сочетании с возможностями технического анализа, обусловленными персонализированной медицинской помощью, сопровождалось правовыми и техническими мерами, обеспечивающими эффективную защиту прав каждого человека, тем более, что основное влияние внедрения ЭЗ видится в качественном изменении системы взаимоотношений медицинского работника и пациента.

Исторически взаимоотношения врача с пациентом определялись, по крайней мере, со стороны врача, нормами врачебной этики и деонтологии, в европейской традиции сформулированными в нескольких фрагментах клятвы Гиппократа: «…Я направлю режим больных к их выгоде сообразно с моими силами и моим разумением, воздерживаясь от причинения всякого вреда и несправедливости… В какой бы дом я ни вошел, я войду туда для пользы больного, будучи далек от всего намеренного, неправедного и пагубного… Что бы при лечении – а также и без лечения – я ни увидел или ни услышал касательно жизни людской из того, что не следует когда-либо разглашать, я умолчу о том, считая подобные вещи тайной…» [2]. Так вводится понятие врачебной тайны – самое известное в обществе понятие врачебной этики, и верность принципу конфиденциальности, как в современной терминологии называ-

ется обязательство сохранения врачебной тайны, отмечается на протяжении всех эпох европейской истории.

С появлением электронных аналогов медицинских документов, и, в особенности, при переходе к электронному документообороту, произошло отчуждение медицинских записей от их источника. В полный рост эта проблема встала при переходе к электронному здравоохранению, включающему персоноцентрический подход к медицинским записям пациента, что предполагает интеграцию данных о здоровье каждого человека в специализированных центрах обработки данных разных уровней. В этом случае появляется возможность доступа к базам данных (БД) медицинских информационных систем (МИС) в течение жизни пациента (и даже после его смерти) не только у лечащего врача и многочисленного медицинского персонала, но и у людей, обеспечивающих техническую поддержку (администраторы баз данных, операторы, обработчики). При возможности трансграничной передачи информации количество лиц, которым она может стать доступна, возрастает многократно. Исходя из этого, возникает проблема сохранения конфиденциальности персональных данных пациента [3], в том числе, и в первую очередь, ДСЗ, то есть любой информации, связанной со здоровьем пациентов, в целях обеспечения его/ее права на личную жизнь, включая право на особый уровень защиты медицинских персональных данных, право на получение информации о своем здоровье, право на контроль доступа к этой информации, право удаления этой информации («право на забвение») и право на участие в принятии решений, касающихся своего здоровья, а также необходимость в жесткой регламентации прав различных групп пользователей на ознакомление с данными пациентов и их коррекцию, то есть уровней доступа к МИС. Решение этой проблемы связано с необходимостью осуществления дополнительных мер по обеспечению неприкосновенности частной жизни пациента и соблюдению врачебной тайны.

Для создания правового поля электронного здравоохранения необходима разработка нормативных правовых актов, регламентирующих [4; 5]:

право на информацию и на свободный доступ к информации, затрагивающей свободы, права, обязанности, интересы личности и организаций, определяющих в целом возможности информационного взаимодействия субъектов общественных отношений;

условия телекоммуникационного обслуживания населения, то есть законодательство, создающее правовую основу для реализации базовых механизмов информационного взаимодействия субъектов в области оказания услуг при использовании современных ИКТ;

формирование электронного документа и (или) ведение электронного документооборота, использование электронной или электронной цифровой подписи, ведение электронной торговли или коммерции, то есть создание правовой основы для информационного взаимодействия субъектов в области оказания услуг ЭЗ, включая услуги телемедицины и использование технологий мобильности;

основы защиты свобод, прав, интересов и безопасности личности в области оказания социально значимых услуг и, в частности, в области оказания услуг ЭЗ (прежде всего, это законодательство о защите прав потребителей, о защите персональных данных, о защите различных законодательно определенных тайн);

предоставление услуг ЭЗ.

При этом, нормы, способствующие развитию ЭЗ, должны касаться следующих вопросов [5]:

государственное регулирование в области ЭЗ, организация системы оказания услуг ЭЗ гражданам, возможные источники и механизмы финансирования таких услуг;

права граждан при оказании им услуг ЭЗ (право граждан на выбор услуг, обязательное информированное согласие на услугу, право на отказ от оказания услуги, право доступа граждан к информации в системе ЭЗ и др.);

требования к лицам, организующим предоставление и предоставляющим услуги ЭЗ, их права и обязанности;

требования к оборудованию и средствам связи, используемым для оказания услуг, требования к документационному сопровождению услуг ЭЗ;

порядок подготовки и сертификации специалистов в области ЭЗ;

порядок создания и функционирования системы автоматизированного учета пациентов, требования к ней и обмену такими данными между медицинскими учреждениями;

возмездное и безвозмездное предоставление услуг ЭЗ, перечень услуг, оказываемых гражданам бесплатно;

обработка и обмен медицинской информацией в сетях связи, соблюдение авторских прав и прав на интеллектуальную собственность при оказании услуг ЭЗ;

международный обмен услугами;

ответственность при организации и предоставлении услуг ЭЗ.

Выполнение работы в рамках научно-прикладного исследования Центра по правам человека при

факультете международных отношений Белорусского государственного университета «Медицинский работник и пациент: взаимодействие в условиях электронного здравоохранения» обусловило ее направленность на изучение сложившейся практики правового регулирования вопросов обеспечения прав человека при оказании услуг ЭЗ в мире (право на выбор услуг, обязательное информированное согласие на услугу, право на отказ от оказания услуги, право собственного доступа и контроля доступа иных лиц (в том числе, медицинских работников) к персональной информации в системе ЭЗ, соблюдение врачебной тайны при свободном обращении ДСЗ и т.д.) с целью разработки предложений по недопущению нарушения этих прав при формировании нормативно-правовой базы ЭЗ в Республике Беларусь.

В первой части работы обобщены результаты исследования международных правовых актов (в частности, актов европейского права) о защите физических лиц при автоматизированной обработке специальных персональных данных, связанных со здоровьем, и о свободном обращении таких данных.

Направленность правового механизма обеспечения прав пациента при внедрении электронного здравоохранения

В Рекомендации CM/Rec (2019) 2 Комитета министров Совета Европы государствам-членам о защите персональных ДСЗ (далее – Рекомендация CM/Rec (2019) 2 [6]), обобщившей почти 40-летний опыт сбора, хранения, автоматизированной обработки и передачи (в том числе, трансграничной) ДСЗ, отмечается, что дополнительными особенностями наблюдаемых за этот период изменений в отношении людей (пациентов) к данным процессам являются их желание обладать большим контролем за использованием персональных ДСЗ и решениями, основанными на обработке таких данных, а также возрастающая вовлеченность пациентов в понимание того, каким образом принимаются касающиеся их решения [6, преамбула, ч.1, абз.8]. В то же время, подтверждается чувствительность ДСЗ для субъекта данных и важность регулирования их использования для гарантии соблюдения фундаментальных прав и свобод каждого человека, в особенности права на защиту частной жизни и персональных данных [6, преамбула, ч.1, абз.10], указывается на принадлежность ДСЗ к специальной категории данных, требующей, в соответствии со статьей 6 Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных №108 [7], более высокого уровня защиты, в частности, из-за риска дискриминации, которая может возникнуть при обработке таких данных [6, преамбула, ч.1, абз.11], и выражается убежденность в том, что каждый человек имеет право на защиту своих ДСЗ, уважение его/ее частной жизни и сохранение конфиденциальности информации, полученной при оказании ему/ей медицинской, то есть оказываемой сертифицированными медицинскими работниками, помощи [6, преамбула, ч.1, абз.12].

В связи с выдвигающимися предположениями о том, что внедрение ЭЗ должно сопровождаться разработкой правового механизма, направленного исключительно или, по крайней мере, в первую очередь на обеспечение прав пациента на получение в доступной для понимания форме полной информации о собственном здоровье, всех проводимых и предлагаемых исследованиях и вмешательствах, возможных альтернативах и последствиях их применения и, в целом, на «медицинское самообразование» пациента, следует подчеркнуть, что в Рекомендации CM/Rec (2019) 2 *разделены две цели внедрения ЭЗ в части автоматизированной обработки ДСЗ – обслуживание субъекта данных* **или** *повышение доступности и качества медицинской помощи и эффективности систем здравоохранения при соблюдении фундаментальных прав каждого человека* [6, преамбула, ч.1, абз.13], при этом, «медицинское самообразование» (и, тем более, самолечение с использованием полученных в сети Интернет советов-«консультаций») к указанным правам не относится, и информирование пациента сверх объема, предусмотренного национальным законодательством («…Информация о состоянии здоровья [сведения о наличии заболевания, диагнозе, возможных методах оказания медицинской помощи, рисках, связанных с медицинским вмешательством, а также возможных альтернативах предлагаемому медицинскому вмешательству] пациента предоставляется лечащим врачом пациенту… Информация о состоянии здоровья пациента излагается лечащим врачом в форме, соответствующей требованиям медицинской этики и деонтологии и доступной для понимания лица, не обладающего специальными знаниями в области здравоохранения… По просьбе несовершеннолетнего либо в целях осознанного выполнения им медицинских предписаний по согласованию с его законным представителем лечащим врачом несовершеннолетнему предоставляется информация о состоянии его здоровья и выбранных методах оказания медицинской помощи в доступной для его возраста форме с учетом психофизиологической зрелости и эмоционального состояния пациента…»

[8, ст.46, ч.1–3, 8]) и Декларацией по защите прав пациента в Европе («…Пациент имеет право на получение полной информации о своем состоянии здоровья, включая данные медицинского обследования, сведения о предполагаемых медицинских вмешательствах, их направленности, потенциальном положительном эффекте и рисках применения каждого вмешательства, наличии альтернатив предлагаемым вмешательствам, включая нелечение, сведения о диагнозе, прогнозе и ходе лечения… Информация должна доводиться до пациента в форме, доступной для его понимания, с минимумом использования медицинской терминологии, с переводом принципиально важных данных на родной язык пациента, если он не владеет государственным…» [9, раздел 2 «Информирование», пп.2.2, 2.4]), не входит в число задач Программы социально-экономического развития Республики Беларусь на 2016–2020 годы [10] по созданию централизованной информационной системы здравоохранения (ЦИСЗ) для формирования единого информационного архива пациентов и обмена медицинскими данными, решаемых при реализации Концепции развития электронного здравоохранения в Республике Беларусь до 2022 года [11], введении понятия и последующем ведении интегрированной электронной медицинской карты (ИЭМК) [12].

Определенное недопонимание при проведении исследований по тематике прав человека при внедрении ЭЗ возникло в связи с отождествлением двух различающихся по субъекту формирования и ведения электронной медицинской карты понятий – ИЭМК (аналог используемого в США понятия Electronic Health Record (EHR; электронная совокупность сведений, связанных со здоровьем субъекта (пациента), соответствующая национальным стандартам совместимости (интероперабельности), которая создается, ведется и используется сертифицированными медицинскими специалистами и персоналом более чем одной организации здравоохранения)), формируемой на государственном уровне, и персональной электронной медицинской карты / персонального электронного медицинского архива (ПЭМК/ПЭМА; аналог используемого в США термина Personal Health Record (PHR; электронная совокупность сведений, связанных со здоровьем субъекта (пациента), соответствующая национальным стандартам совместимости (интероперабельности), полученная из различных источников, в том числе, внесенная самим пациентом, ведение, управление и предоставление доступа к которым осуществляет сам субъект (пациент), или, по соглашению с пациентом, хранение и предоставление сервиса ведения и управления ПЭМК осуществляет специализированный провайдер)), формируемой самим пациентом для личного использования, включая и цели «медицинского самообразования» [13–15].

Регулирование отношений, связанных с обращением персональных данных, включая специальные персональные данные, связанные со здоровьем, в международном праве

Юридические основы права на защиту частной жизни (в том числе, и персональных данных как составляющей личной тайны) были установлены Всеобщей декларацией прав человека, а также Европейской конвенцией о защите прав человека и основных свобод.

В соответствии со статьей 12 Всеобщей декларации прав человека никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств [16].

Статья 8 Европейской конвенции о защите прав человека и основных свобод устанавливает, что каждый имеет право на уважение его личной и семейной жизни, жилища и корреспонденции [17].

Положения Всеобщей декларации прав человека в части декларации неприкосновенности частной жизни были также закреплены в статье 17 Международного пакта о гражданских и политических правах, одобренного резолюцией Генеральной Ассамблеи ООН от 16 декабря 1966 г. №2200 А (XXI), согласно которой никто не может подвергаться произвольному или незаконному вмешательству в личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну корреспонденции либо незаконным посягательствам на честь и репутацию. Каждый человек имеет право на защиту от такого вмешательства или посягательства [18].

Право на неприкосновенность частной жизни имплементировано конституционным законодательством всех европейских государств. Статья 28 Конституции Республики Беларусь также предусматривает, что каждый человек имеет право на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство [19].

Вместе с тем, объективные причины современного социального взаимодействия в условиях единого информационного пространства и прогрес-

са социальных технологий потребовали дополнительной регламентации в области обеспечения неприкосновенности личной жизни граждан, в том числе при автоматизированной обработке персональных данных.

В течение двух последних десятилетий законодательными органами Европейского союза принято значительное число нормативных актов, направленных на регламентацию вопросов получения, обработки и обращения с персональными данными и информацией о личной жизни.

Установлено, что поскольку системы обработки данных предназначены для службы человеку, следовательно, эти системы должны соблюдать основные права и свободы, в том числе, право на неприкосновенность частной жизни. При этом, уровень защиты прав и свобод граждан при обработке персональных данных должен быть равноценным во всех государствах - членах Европейского союза, так как данная цель не может быть достигнута усилиями отдельных государств.

Первым специальным международным документом, направленным на регламентацию обращения и защиты персональных данных в мировом сообществе, и признанным международным стандартом является Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных №108, заключенная в г. Страсбурге 28 января 1981 г. (далее – **Конвенция 108**) [7].

Цель Конвенции 108 – обеспечение на территории всех участников для каждого человека, независимо от его гражданства или места жительства, уважения его прав и основных свобод и, в частности, его права на неприкосновенность частной жизни в отношении автоматизированной обработки касающихся его персональных данных («защита данных»).

Конвенцией 108 сформулирован следующий понятийный аппарат:

персональные данные – любая информация об определенном или поддающемся определению (могущем быть идентифицированным) физическом лице (субъект данных);

автоматизированная база данных – любой набор данных, подвергающихся автоматизированной обработке;

автоматизированная обработка – операции, осуществляемые полностью или частично с помощью автоматизированных средств, включая: хранение данных, осуществление логических и/или арифметических операций с этими данными, их изменение, уничтожение, поиск или распространение;

контролер базы данных – означает физическое или юридическое лицо, орган государственной власти, учреждение или любой другой орган, компетентный в соответствии с внутренним законодательством решать, какова должна быть цель создания автоматизированной базы данных, какие категории персональных данных подлежат хранению или какие операции должны производиться с ними.

Каждое из государств – участников обязалось принять необходимые меры для того, чтобы основные принципы защиты данных, изложенные в Конвенции, были реализованы в его национальном праве (часть 1 статьи 4).

Статья 5 содержит требования к качеству данных, а именно:

персональные данные, подвергающиеся автоматизированной обработке:

собираются и обрабатываются на справедливой и законной основе;

хранятся для определенных и законных целей и не используются иным образом, несовместимым с этими целями;

являются адекватными, относящимися к делу и не чрезмерными для целей их хранения;

являются точными и, когда это необходимо, обновляются;

сохраняются в форме, позволяющей идентифицировать субъекты данных, не дольше, чем это требуется для целей хранения этих данных.

Выделены специальные категории данных (персональные данные, касающиеся расовой принадлежности, политических взглядов или религиозных или других убеждений, а также *персональные данные, касающиеся здоровья* или половой жизни, судимости, которые не могут подвергаться автоматизированной обработке, если внутреннее законодательство не устанавливает соответствующих гарантий (статья 6).

Таким образом, вводятся такие основополагающие принципы защиты персональных данных, как ограничение на обработку персональных данных о национальной принадлежности, политических взглядах либо религиозных или иных убеждениях, в том числе персональных данных, касающихся здоровья или сексуальной жизни лица, его судимости.

Определено, что для защиты персональных данных, хранящихся в автоматизированных базах данных, принимаются надлежащие меры безопасности, направленные на предотвращение их случайного или несанкционированного уничтожения или случайной потери, а также на предотвращение несанкционированного доступа, их изменения или распространения таких данных (статья 7).

Основные права субъекта персональных данных включают (статья 8):

право на информацию о существовании автоматизированной базы персональных данных, о ее главных целях, а также о контролере базы данных, его месте жительства либо юридическом адресе;

право на получение информации о том, накапливаются ли в автоматизированной базе данных касающиеся его персональные данные, и какие именно;

право требования уточнения или уничтожения данных, если они были обработаны с нарушением положений национального права, реализующих основные принципы, изложенные в Конвенции;

право на судебную защиту в случае, если его запрос либо требование о предоставлении информации, уточнении или уничтожении данных не были удовлетворены.

Отступление от положений статей 5, 6 и 8 допускается только в случае, если это предусмотрено внутренним законодательством и является необходимой в демократическом обществе мерой, принимаемой в интересах:

защиты безопасности государства, общественной безопасности, валютно-кредитных интересов государства или пресечения уголовных преступлений;

защиты субъекта данных или прав и свобод других лиц;

а также в отношении автоматизированных баз персональных данных, используемых для целей статистики или научных исследований, когда явно отсутствует какой-либо риск нарушения неприкосновенности частной жизни субъектов данных.

Статья 12 содержит положения о регулировании трансграничных потоков персональных данных, подвергающихся автоматизированной обработке или собранных с целью их автоматизированной обработки.

Существенно, что в отношении положений Конвенции не может делаться никаких оговорок (статья 25).

В настоящее время Конвенцию 108 подписали 47, ратифицировали 55 стран, среди которых присутствуют государства, не являющиеся членами Совета Европы – Аргентина, Мексика, Марокко, Тунис, Уругвай и др.

8 ноября 2001 г. в г. Страсбурге был подписан дополнительный Протокол к Конвенции 108 о наблюдательных органах и трансграничной передаче информации ETS 181 (далее – дополнительный **Протокол ETS 181**) [20].

Данным международным договором регламентированы вопросы создания и функционирования в странах, подписавших и ратифицировавших Конвенцию 108, наблюдательных органов, которые несут ответственность за соблюдение ограничений национального права в целях реализации принципов, заложенных в Конвенции.

Дополнительный Протокол ETS 181 устанавливает, что данные органы независимы в осуществлении своих функций и уполномочены проводить расследования, принимать участие в юридических процессах, акцентировать внимание компетентных судебных органов на нарушениях национального права, обеспечивающего реализацию защиты персональных данных. Кроме того, наблюдательные органы рассматривают претензии, поданные любым лицом и связанные с защитой его прав и фундаментальных свобод в отношении обработки персональных данных.

Помимо регламентации вопросов создания и функционирования наблюдательных органов, дополнительный Протокол ETS 181 определяет основы трансграничной передачи персональных данных, осуществляемой между двумя и более государствами.

10 октября 2018 г. в г. Страсбурге подписан Протокол о внесении изменений в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных №223 (далее – **Протокол 223**) [21].

Положения Протокола 223 после его ратификации станут неотъемлемой частью новой редакции Конвенции 108, расширяя и дополняя действующий с 1981 г. международный договор, предоставляя правовые механизмы защиты персональных данных, в том числе при их трансграничной передаче. В этом случае конвенция сможет защитить законные интересы субъектов персональных данных от транснациональных IT-компаний, которые стремятся распространить правила обработки персональных данных, принятые в своей национальной юрисдикции, на страны, где они ведут бизнес.

В преамбуле новой редакции Конвенции 108 содержится призыв учитывать диверсификацию, интенсификацию и глобализацию обработки данных и потоков персональных данных, право человека контролировать персональные данные и их обработку («принцип личной автономии»).

Целью Конвенции в новой редакции является защита каждого человека, вне зависимости от его национальности или места жительства, при автоматической обработке его/ее персональных данных, способствуя, тем самым, соблюдению в отношении него/нее фундаментальных прав и свобод человека, в особенности, права на частную жизнь.

Определение обработки данных охватывает более широкий комплекс операций с персональ-

ными данными по сравнению с действующей конвенцией, включая их сбор, обеспечение сохранности, извлечение, обнародование, обеспечение доступности и удаление.

Вводятся понятия «контролер» (физическое или юридическое лицо, орган государственной власти, служба, агентство или любой другой орган, который самостоятельно или совместно с другими лицами (органами) имеет полномочия на принятие решений в отношении обработки персональных данных), «получатель» (физическое или юридическое лицо, орган государственной власти, служба, агентство или любой другой орган, которому раскрываются или становятся доступными персональные данные) и «лицо, осуществляющее обработку данных» (физическое или юридическое лицо, орган государственной власти, служба, агентство или любой другой орган, осуществляющие обработку персональных данных от имени (по поручению) контролера).

Положения Конвенции распространяются на обработку персональных данных в рамках национальных юрисдикций для всех физических лиц независимо от их гражданства или места жительства, включая иностранных лиц, лиц без гражданства и иных субъектов данных, обратившихся в компетентные органы государства-участника конвенции за защитой своих персональных данных.

В сферу применения Конвенции входит обработка данных в организациях любой формы собственности, однако ее действие не распространяется на обработку данных, осуществляемую физическим лицом для сугубо личных или бытовых надобностей.

Статья 5 Конвенции (имеющая в новой редакции наименование «Законность обработки и качество данных») определяет, что:

«1. Обработка данных должна быть пропорциональна преследуемым законным целям и предусматривать на всех стадиях справедливый баланс между интересами всех заинтересованных сторон, вне зависимости от того, являются ли они государственными или частными структурами, и правами и свободами человека.

2. Каждая Сторона обязана обеспечить, чтобы обработка данных осуществлялась на основе свободного, ясно выраженного, информированного и недвусмысленного согласия субъекта данных или на основе других указанных в законодательстве оснований.

3. Подвергаемые обработке персональные данные должны обрабатываться законным образом.

4. Подвергаемые обработке персональные данные должны быть:

a) обработаны честным и прозрачным способом;

b) собраны с точной, конкретной и законной целью и не обрабатываться способом, который несовместим с этими целями; дальнейшая обработка информации для достижения целей в общественных, исторических или научных, статистических сферах должна сопровождаться соответствующими гарантиями, совместимыми с этими целями;

c) адекватными, актуальными и представленными в объеме, не превышающем цели, для которых они обрабатываются;

d) точными и, если необходимо, обновляемыми;

e) сохраненными в форме, которая позволяет идентификацию субъекта данных в объеме, не превышающем необходимый уровень для достижения целей, ради которых персональные данные обрабатываются.».

Обязательства государств обеспечивать обработку данных на основе добровольного, четко выраженного, информированного и однозначного согласия субъекта данных являются дополнительными по сравнению с действующей редакцией Конвенции 108.

Расширен перечень данных, обработка которых отнесена к «специальной категории данных» и может быть осуществлена только в том случае, если законом установлены соответствующие гарантии. Теперь к ним дополнительно отнесены генетические данные, биометрические данные, персональные данные, касающиеся правонарушений, уголовного судопроизводства, а также связанных с ними мер безопасности (статья 6 новой редакции Конвенции).

Конвенция уполномочивает контролера своевременно уведомлять компетентный надзорный орган об утечках данных, которые могут привести к серьезным нарушениям прав и основных свобод субъектов данных (статья 7 новой редакции).

В соответствии с вводимой статьей 8 «Прозрачность обработки данных», государства должны обеспечить, чтобы контролер информировал субъекта о подвергаемых обработке персональных данных (паспортные данные, место жительства), правовых основаниях и целях обработки данных, категориях обрабатываемых персональных данных, получателях данных, мерах обеспечения прав субъекта данных, указанных в статье 9 новой редакции Конвенции, а именно:

право на принятие решения по обработке его/ее персональных данных только с учетом его/ее мнения;

право на получение по запросу в разумный временной интервал, без чрезмерной задержки или

затрат, в понятной форме подтверждения обработки его/ее персональных данных, информации об обрабатываемых данных, всей доступной информации об источнике персональных данных, информации о времени хранения соответствующих сведений и любой другой информации, которую контролер должен предоставить для обеспечения прозрачности обработки данных в соответствии со статьей 8;

право на получение по запросу сведений, обосновывающих необходимость обработки данных, в случае, если результаты подобной обработки затрагивают его/ее частную жизнь;

право на обращение в любое время, по личным причинам с беспокоящими его/ее вопросами, связанными с обработкой персональных данных, если контролер не предоставляет информацию о законных основаниях обработки данных и подобная обработка нарушает фундаментальные права и свободы человека;

право (при обращении) на исправление или удаление данных (бесплатно и в разумные сроки), если они были обработаны с нарушением положений Конвенции;

право на правовую защиту, в соответствии со статьей 12 Конвенции, если его/ее права в соответствии с данной Конвенцией были нарушены;

право (вне зависимости от его/ее национальности или места жительства) на помощь со стороны надзорного органа, указанного в статье 15 Конвенции, в осуществлении его/ее прав в соответствии с данной Конвенцией.

В соответствии со статьей 10 новой редакции «Дополнительные обязательства», государства – участники обязаны обеспечить:

соблюдение со стороны контролера и, при необходимости, лиц, осуществляющих обработку данных, всех обязательств в рамках данной Конвенции, что может быть подтверждено надзорным органом, указанным в статье 15 Конвенции;

оценку контролером и, при необходимости, лицами, осуществляющими обработку данных, потенциального воздействия предполагаемой обработки персональных данных на фундаментальные права и свободы субъекта данных до начала подобной обработки, и осуществление процесса обработки данных таким образом, чтобы предотвратить или минимизировать риск нарушения этих фундаментальных прав и свобод;

реализацию контролером и, при необходимости, лицами, осуществляющими обработку данных, технических и организационных мер, учитывающих необходимость соблюдения права на защиту персональных данных на всех стадиях их обработки.

Вопросы обработки персональных данных, относящихся к сведениям, составляющим государственную тайну, фактически выведены за скобки новой редакции Конвенции.

Конвенция допускает исключения и ограничения по такой категории данных (статья 11) в случаях защиты национальной безопасности, обороны, общественной безопасности, общественных интересов, важных экономических и финансовых интересов государства, обеспечения беспристрастности и независимости судебной власти, предотвращения, расследования и наказания преступлений, исполнения наказания по уголовным делам, а также для защиты субъекта данных или прав и основных свобод других лиц.

Вопросы, связанные с государственной тайной, не будут рассматриваться при мониторинге выполнения Конвенции, при осуществлении трансграничной передачи данных и в деятельности предусмотренных Конвенцией национальных надзорных органов.

Появляются новые требования в отношении обработки данных в целях архивации в общественных интересах, научных, историко-исследовательских или статистических целях.

В вопросе о трансграничной передаче персональных данных в новой редакции Конвенции подтверждается положение о том, что государства не должны запрещать или обусловливать выдачей специального разрешения передачу таких данных получателю, находящемуся в юрисдикции другого государства, единственно с целью защиты персональных данных (статья 14).

Однако, учитывая возрастающую угрозу экстерриториального применения законодательства ряда стран, легализующих доступ своих транснациональных компаний и правоохранительных органов к персональным данным граждан других стран (CLOUD Act), государства-члены Совета Европы согласились отказаться от трансграничной передачи персональных данных, если имеется реальный и серьезный риск того, что передача данных другому государству или от упомянутого другого государства стране, не являющейся участницей Конвенции, приведет к несоблюдению ее положений.

В новой редакции Конвенции вводится требование учредить один или несколько надзорных органов, ответственных за ее выполнение, с четким описанием их полномочий.

В частности, надзорные органы уполномочены проводить расследования, выносить решения в отношении нарушений положений Конвенции, накладывать административные штрафы, принимать участие в судебном процессе, предоставлять консуль-

тации относительно предложений о разработке любых законодательных или административных актов в области обработки персональных данных, рассматривать запросы и жалобы субъектов данных, а также запрещать, приостанавливать или ограничивать трансграничную передачу данных в целях защиты прав и основных свобод субъектов данных.

В своей работе надзорные органы должны быть полностью независимыми и действовать беспристрастно, не запрашивая и не получая указаний, при должном финансировании, позволяющем эффективно выполнять свои функции.

Предусмотрено учреждение комитета сторон – органа, уполномоченного проводить выездные проверки, оценивать степень выполнения Конвенции и выносить рекомендации о более эффективной реализации государствами ее требований.

Помимо мониторинга, в задачи комитета сторон входят вопросы толкования и применения Конвенции, внесения поправок и содействия в урегулировании разногласий между государствами.

Комитет сторон конвенции созывается Генеральным секретарем Совета Европы через год после вступления конвенции в силу.

Итоги каждого заседания, которые проводятся не реже одного раза в год, комитет сторон докладывает комитету министров Совета Европы.

Каждое государство назначает в комитет сторон представителя и его заместителя, которые уполномочены голосовать (каждое государство имеет один голос).

Решения по вопросам, относящимся к деятельности комитета сторон (статья 23), принимаются большинством в четыре пятых голосов, а по докладам о выполнении государствами положений конвенции (пункт h статьи 23) – большинством в четыре пятых, включая большинство голосов государств, не являющихся членами организации региональной интеграции (Европейский союз), которая является участницей конвенции.

Такой высокий количественный показатель для голосования (80%) предложен для обеспечения равноправного участия всех государств – участников Конвенции в принятии решений, без каких-либо попыток блокового голосования со стороны ЕС от имени всех своих государств.

По-прежнему не допускаются оговорки (односторонние заявления принявших Конвенцию государств, сделанные с целью оговорить условия, при которых государство не будет соблюдать положения Конвенции) в отношении Конвенции.

Применительно к собственно медицинским данным или, шире, данным, связанным со здоровьем (ДСЗ), относящимся к специальным персональным данным, для которых, в соответствии со статьей 6 Конвенции 108, требуется более высокий уровень защиты, в частности, из-за риска дискриминации, к которой может привести их обработка, 27 марта 2019 г. на 1342-м заседании заместителей министров принята Рекомендация CM/Rec (2019) 2 Комитета министров Совета Европы государствам-членам о защите персональных ДСЗ (далее – **Рекомендация CM/Rec (2019) 2**) [6].

В дополнение к указанным в Конвенции 108 и Протоколе 223, в Рекомендации CM/Rec (2019) 2 содержатся определения следующих терминов:

анонимизация – обработка персональных данных с целью обеспечения того, чтобы субъект данных не мог быть идентифицирован прямым или косвенным образом;

псевдонимизация – обработка персональных данных таким образом, чтобы субъект данных не мог быть идентифицирован без использования дополнительной информации, получаемой не в процессе сбора персональных данных, и при условии, что применяются технические и организационные средства для обеспечения того, чтобы соответствующая личная информация не ассоциировалась с идентифицированным лицом;

персональные данные, связанные со здоровьем человека (ДСЗ) – любые персональные данные, касающиеся физического или психического здоровья конкретного лица, включая данные, полученные при оказании медицинских услуг, позволяющие иметь данные о состоянии здоровья человека в прошлом, в настоящее время, а также прогнозировать изменения в состоянии здоровья в будущем.

В главе 2 Рекомендации CM/Rec (2019) 2 «Правовые основания обработки ДСЗ» определены следующие принципы обработки этих данных (п.4):

ДСЗ должны обрабатываться прозрачным, законным и честным образом (пп.4.1.a);

ДСЗ должны собираться в четко обозначенных и законных целях и не должны обрабатываться таким образом, который несовместим с этими целями; дальнейшая передача этих данных в государственных, научных интересах, для проведения ретроспективных исследований или получения статистической информации возможна при соблюдении фундаментальных прав и свобод человека (пп.4.1.b);

обработка данных должна быть необходимой и пропорциональной при реализации поставленной законной цели и может осуществляться только на основе согласия субъекта данных или на других законных основаниях (пп.4.1.c);

персональные данные должны, в той степени, в которой это возможно, быть получены от субъекта данных; в тех случаях, когда субъект данных не в состоянии их предоставить, а они являются

необходимыми, данные могут быть собраны из других источников (пп.4.1.d);

данные должны быть адекватными, уместными и собираться в объеме, соответствующем целям их обработки; данные должны быть точными и, при необходимости, актуализироваться (пп.4.1.e);

для предотвращения рисков (случайный и неавторизированный доступ к ДСЗ, их уничтожение, утрата, несанкционированное использование, неготовность, недоступность, модификация, раскрытие) должны применяться соответствующие средства защиты информации (пп.4.1.f);

при обработке данных должны соблюдаться права субъекта данных, в первую очередь, на доступ к информации, уточнение и удаление данных, возражение против обработки ДСЗ (пп.4.1.g).

Принципы защиты ДСЗ должны учитываться по умолчанию (конфиденциальность по умолчанию – privacy by default) и быть предусмотрены непосредственно при создании МИС, в которых обрабатываются ДСЗ (предусмотренная конфиденциальность – privacy by design) (пп.4.2).

Контролеры и лица, осуществляющие обработку данных, не являющиеся медицинскими работниками, должны соблюдать требования конфиденциальности и безопасности на уровне, эквивалентном требуемому от медицинских работников (пп.4.4).

Установлены законные основания для обработки ДСЗ (пп.5a):

оказание медицинской и медико-социальной помощи медицинскими и социальными работниками (предоставление услуг по профилактике, диагностике, лечению и медицинской реабилитации):

реализация целей общественного здравоохранения, реализация действий гуманитарного характера, обеспечение высокого стандарта качества и безопасности медицинской помощи, включая обеспечение лекарственными средствами и медицинскими изделиями;

защита жизненно важных интересов субъекта данных или другого лица, если согласие субъекта данных не может быть получено;

реализация целей, связанных с обязательствами контролера, для осуществления их прав или прав субъекта данных в части трудоустройства и социальной защиты;

решение социально значимых задач в сфере медицины, проведения научных, статистических исследований;

реализация действий, вытекающих из признания требований по судебному иску, выполнение требований истца или защиты в суде;

в случаях, представляющих существенный общественный интерес.

ДСЗ могут обрабатываться, если субъект данных предоставил свое согласие, за исключением тех случаев, когда законодательство предусматривает, что запрет на обработку ДСЗ не может быть снят исключительно на основе согласия субъекта данных. В случаях, когда, в соответствии с законодательством, требуется согласие субъекта данных на обработку ДСЗ, оно должно быть добровольным, конкретно выраженным, сделанным на основе получения всей необходимой информации. Субъект данных должен быть проинформирован о своем праве отозвать свое согласие на обработку данных в любой момент, а также уведомлен, что подобный отзыв согласия не влияет на правомерность обработки данных, осуществленной до момента отзыва субъектом данных согласия на их обработку. При этом, отзыв согласия на обработку данных должен быть такой же простой процедурой, как и его предоставление (пп.5b).

ДСЗ могут обрабатываться, если это требуется в рамках договора на оказание медицинской помощи, и в этом договоре оговорены условия обработки данных, включающие соблюдение их конфиденциальности и сохранения врачебной тайны (пп.5c).

Могут обрабатываться ДСЗ, сознательно сделанные публичными субъектом данных (пп.5d).

При всех условиях, должны быть обеспечены соответствующие гарантии безопасности при обработке ДСЗ и соблюдены права человека (пп.5e).

Субъект данных имеет право на ознакомление с любой касающейся ДСЗ информацией. При этом, он/она может иметь свои собственные причины не желать знать об определенных аспектах собственного здоровья, и, до проведения любого исследования/обследования, все должны быть осведомлены о возможности не быть информированными об их результатах, включая случаи, когда результаты оказались неожиданными. Желание субъектов данных не иметь информацию о собственном здоровье может, в определенных обстоятельствах, быть ограничено, как это предусмотрено в законодательстве, если это необходимо для реализации собственных интересов субъекта данных или для реализации обязанностей врача по оказанию медицинской помощи (пп.7.6).

В случаях, когда обмен ДСЗ происходит между различными медицинскими работниками при предоставлении медицинской помощи конкретному лицу, субъект данных должен быть заранее проинформирован об этом, за исключением случаев, когда предоставление подобной информации невозможно из-за чрезвычайной ситуации или

когда субъект данных уже обладает этой информацией (подпункт 8.1). В тех случаях, когда обмен информацией осуществляется на основе согласия субъекта данных, это согласие может быть отозвано в любой момент в соответствии с подпунктом 5b. Если обмен данными предусмотрен законодательством, субъект может возражать против обмена его ДСЗ.

Медицинские работники, непосредственно занимающиеся оказанием медицинской помощи и вопросами социального обеспечения конкретного лица, осуществляющие обмен данными в целях достижения более высокого уровня преемственности и обеспечения качества медицинской помощи, должны соблюдать врачебную тайну (подпункт 8.2).

Обмен данными между медицинскими работниками должен быть ограничен информацией, необходимой для обеспечения преемственности или непрерывности лечебно-диагностического процесса. Соответствующие медицинские работники могут, в этом случае, только распределять или получать информацию в пределах своей компетенции и в зависимости от наличия у них разрешения на получение той или иной информации (подпункт 8.3).

В соответствии с этими принципами используются электронные медицинские файлы и электронная почта для обмена ДСЗ (подпункт 8.4).

При обмене ДСЗ должны быть предприняты физические, технические и административные меры безопасности, так же как и меры, необходимые для гарантирования конфиденциальности, целостности и доступности ДСЗ (подпункт 8.5).

Установлены ограничения доступа к ДСЗ отдельных категорий потребителей, не связанных с оказанием МП (п.9).

В любом случае, доступ к ДСЗ может быть обеспечен только тем категориям потребителей, которые определены законодателем (пп.9.1).

Страховые компании не могут иметь права на доступ к ДСЗ, касающимся конкретного лица, если соответствующие гарантии не предусмотрены в законодательстве (подпункт 9.2).

Работодатели не могут иметь права на доступ к ДСЗ, касающимся конкретного лица, за исключением приема на работу (подпункт 9.3).

ДСЗ могут передаваться только авторизованному получателю, который соблюдает правила конфиденциальности, обязательные для медицинского работника (подпункт 9.4).

Установлены ограничения по срокам хранения ДСЗ. Они не должны храниться в форме, которая позволяет получать сведения о субъекте данных в течение более длительного периода времени, чем это предусмотрено целями обработки ДСЗ, за исключением случаев, когда ДСЗ используются для проведения научных, ретроспективных и статистических исследований. В последнем случае осуществляется максимально возможная анонимизация данных (пункт 10).

Глава 3 Рекомендации CM/Rec (2019) 2 «Права субъекта данных» включает пункты 11 (Транспарентность обработки ДСЗ) и 12 (Права субъекта персональных ДСЗ (пациента) на доступ, использование, корректировку и удаление ДСЗ).

Так, контролер должен информировать субъекта данных об обработке касающихся его/ее ДСЗ (пп.11.1).

Эта информация должна включать (пп.11.2):

контактные данные контролера и уполномоченного лица (обработчика) в тех случаях, когда это необходимо;

цель обработки ДСЗ (в тех случаях, когда на это существуют соответствующие правовые основания);

длительность хранения ДСЗ;

наименование получателей или категорий получателей ДСЗ; сведения о ДСЗ, запланированных для передачи третьей стране или международной организации;

разъяснения относительно возможности субъекта данных возражать против обработки касающихся его ДСЗ, в соответствии с условиями, указанными в пп.12.2;

механизмы, доступные субъекту данных, для осуществления через контролера его/ее прав на доступ, уточнение или уничтожение касающихся его ДСЗ.

В тех случаях, когда это необходимо для честной и прозрачной обработки ДСЗ, информация также должна включать (пп.11.3):

уведомление субъекта данных о том, что касающиеся его ДСЗ могут быть обработаны в определенных законодательством целях с соблюдением предусмотренных мер безопасности и в соответствии с условиями, указанными в пп.4.1.b;

уведомление о возможности подачи жалобы в надзорный орган;

уведомление о возможности автоматизированного процесса принятия решения, включая профайлинг, при обработке ДСЗ (только в случаях, указанных в законодательстве и при соблюдении необходимых мер безопасности).

Необходимая информация должна быть предоставлена субъекту данных до начала сбора информации или при первом контакте с ним (пп.11.4).

Информация должна быть понятной и легко оцениваемой, должна быть четко сформулирована и предоставлена субъекту данных в доступной его

пониманию форме, позволяющей полностью понять механизм предстоящей обработки информации. В случае законодательно установленной недееспособности субъекта данных, информация должна быть предоставлена его законному представителю. Если признанное недееспособным лицо (субъект данных) способно понимать информацию, данное лицо также должно быть проинформировано до начала обработки информации (пп.11.5).

Контролер не обязан предоставлять данную информацию в тех случаях, когда субъект данных уже имеет необходимую информацию. Более того, в тех случаях, когда персональные ДСЗ не получены напрямую от субъекта данных, контролер не обязан информировать субъекта данных об обработке ДСЗ, если данная обработка предусмотрена законодательством или сообщить об обработке ДСЗ субъекту невозможно, например, вследствие того, что контактные данные субъекта изменились и из-за этого субъект ДСЗ не может быть найден, или вследствие того, что передача данных требует от контролера непропорциональных усилий, в особенности, при обработке информации для решения общественно важных задач или в научных, исторических и статистических целях (пп.11.7).

Желание субъекта данных не быть проинформированным о поставленном ему диагнозе или прогнозе состояния его здоровья должно быть соблюдено, за исключением тех случаев, когда подобные действия представляют серьезный риск для здоровья других лиц (пп.11.7).

Контролер не обязан предоставлять информацию субъекту данных в тех случаях, когда это предусмотрено законодательством и является необходимым и пропорциональным решением в демократическом обществе для достижения целей, указанных в статье 9 Конвенции 108 (пп.11.8).

Права субъекта персональных ДСЗ (пациента) на доступ, использование, корректировку и удаление ДСЗ определены в п.12.

Субъект данных имеет право знать, обрабатываются ли его персональные данные, и в случае, если такая обработка происходит, получить эти данные без чрезмерной задержки или расходов и в понятной форме, а также получить информацию о целях обработки данных, категориях обрабатываемых данных, получателе (получателях) данных, данных, подлежащих передаче третьей стране или международной организации, периоде хранения данных, причинах, послуживших основанием для обработки ДСЗ (подпункт 12.1).

В подпункте 12.2:

подтверждено право субъекта на удаление данных, обработка которых осуществляется в нарушение Конвенции 108, а также право на исправление собственных ДСЗ;

установлено, что субъект данных имеет право возражать по основаниям, связанным с его личными обстоятельствами, против обработки его ДСЗ, кроме случаев, когда такая обработка осуществляется на анонимной основе, или контролер представил обоснованную причину обработки ДСЗ.

В случае, если требования субъекта данных об исправлении или удалении ДСЗ или его/ее возражения отклонены, у субъекта данных должна быть возможность оспорить подобные решения в судебном порядке (подпункт 12.3).

Субъект данных должен иметь право на участие в принятии решения об обработке собственных ДСЗ (подпункт 12.4).

При автоматизированной обработке данных, субъект данных должен иметь возможность получить от контролера в структурированном, интероперабельном и машиночитаемом формате собственные ДСЗ с целью передачи ее другому контролеру (переносимость данных). Субъект данных должен иметь возможность требовать от контролера передавать информацию напрямую другому контролеру (подпункт 12.5).

Права субъекта данных должны восприниматься медицинскими работниками как часть профессиональной этики (подпункт 12.6).

Должны предоставляться соответствующие законодательные гарантии защиты прав субъекта данных (подпункт 12.8).

В пунктах 13 и 14 содержатся требования к безопасности и интероперабельности систем обработки данных (целостность, проверяемость данных, отслеживание доступа, обеспечение переносимости данных).

Определены требования к системам сбора и обработки данных на мобильных устройствах (пункт 16).

Для облегчения адаптации положений Конвенции 108 применительно к нормам национального законодательства государств, являющихся ее участниками, Европейская комиссия выступила с инициативой гармонизации законодательства стран Европейского союза в сфере защиты персональных данных путем принятия ряда **директив Европейского парламента и Совета Европейского союза**.

Так, 24 октября 1995 г. Европейским Парламентом и Советом Европейского Союза принята **Директива 95/46/ЕС** о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (в редакции Регламента Европейского парламента и Совета Ев-

ропейского союза от 29 сентября 2003 года №1882/2003) [22], установившая единство принципа свободы обращения персональных данных между государствами-членами ЕС и принципа защиты права физических лиц на неприкосновенность частной жизни при обработке их персональных данных.

Каждое государство – член Европейского союза применяет к обработке персональных данных национальные нормы, которые принимаются в соответствии с названной Директивой. Причем, под персональными данными следует понимать любую информацию, относящуюся к определенному физическому лицу. При этом, часть 20 преамбулы Директивы 95/46/ЕС устанавливает, что факт осуществления обработки данных лицом, учрежденным в третьей стране, не должен препятствовать защите физических лиц, предусмотренной в Директиве. В таких случаях обработка должна регулироваться законодательством государства-члена ЕС, в котором находятся средства, используемые для обработки данных, и должны обеспечиваться гарантии фактического уважения прав и обязанностей, предусмотренных Директивой. Аналогичные положения содержатся в статье 4 Директивы 95/46/ЕС.

Определение понятия персональных данных содержится в статье 2 вышеуказанной Директивы. Согласно данной норме, под персональными данными понимается любая информация, относящаяся к определенному или определяемому физическому лицу (субъекту данных); определяемым является лицо, которое может быть определено прямо или косвенно, в частности, через идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Обработка персональных данных означает любую операцию или последовательность операций, осуществляемых с этими данными, с использованием автоматических средств или без таковых, таких как сбор, запись, организация, хранение, модификация или замена, извлечение, консультирование, использование, раскрытие через передачу, распространение или предоставление доступа другим способом, блокирование, стирание или разрушение. Оператором является физическое или юридическое лицо, государственный орган, агентство или любой другой орган, который самостоятельно или совместно с другими определяет цели и способы обработки персональных данных.

Параграф 1(e) статьи 6 Директивы 95/46/ЕС устанавливает, что персональные данные должны храниться в форме, позволяющей проводить идентификацию субъектов данных не дольше, чем это необходимо для целей, с которыми они были собраны или в дальнейшем обработаны. Хранение в течение более долгих сроков возможно в исторических, статистических или научных целях с соблюдением установленных на государственном уровне гарантий.

Обработка персональных данных возможна при обязательном наличии одного из следующих условий (статья 7):

однозначного согласия субъекта данных;

необходимости обработки данных для исполнения договора, стороной которого является субъект данных или в целях принятия мер по просьбе субъекта данных до заключения договора;

необходимости обработки данных для соблюдения юридического обязательства, субъектом которого является оператор;

необходимости обработки данных в целях защиты жизненно важных интересов субъекта данных;

необходимости обработки данных для выполнения задачи, осуществляемой в общественном интересе, или при исполнении официальных правомочий, возложенных на оператора или третье лицо, которому раскрываются данные;

необходимости обработки данных для целей законных интересов, преследуемых оператором или третьим лицом, которому раскрываются данные, за исключением случаев, когда перед такими интересами имеют преимущество интересы, связанные с основными правами и свободами субъекта данных.

При этом, параграф 1 статьи 8 Директивы 95/46/ЕС содержит запрет на обработку персональных данных, касающихся состояния здоровья или половой жизни физического лица, равно как раскрывающих его расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения, членство в профсоюзах. Исключением являются особо оговоренные ситуации, например, когда обработка данных требуется для целей профилактической медицины, медицинской диагностики, оказания медицинской помощи или лечения, либо управления здравоохранением, и когда эти данные обрабатываются медицинским работником согласно национальному законодательству или правилам, установленным компетентными национальными органами в отношении обязанности хранения профессиональной тайны или иным лицом, также ограниченным равноценным обязательством хранения тайны.

25 мая 2018 г. вступило в силу постановление Европейского парламента и Совета ЕС 2016/679 от 27 апреля 2016 г. «О защите физических лиц при обработке персональных данных и о свобод-

ном обращении таких данных, и отмене Директивы ЕС 95/46 (Регламент ЕС по защите персональных данных)» (далее – **РЗПД**) [23].

Принятие РЗПД направлено на усиление и унификацию защиты персональных данных всех лиц на территории ЕС, регулирование трансграничного обмена этими данными как между странами ЕС, так и государствами, не входящими в Европейский союз.

В соответствии с нормами РЗПД, граждане в полной мере обладают функцией контроля над собственными персональными данными, также путем унификации регулирования в рамках ЕС значительно упрощена нормативная база международных экономических отношений.

В рамках РЗПД подтверждены и, во многом, конкретизированы ключевые принципы защиты персональных данных, принятые мировым (европейским) сообществом и отраженные в Конвенции 108 в редакции Протокола 223, Протоколе ETS 181 и утратившей силу в связи с принятием данного Регламента Директиве ЕС 95/46:

законность, справедливость и прозрачность (наличие легальных оснований для сбора и использования данных в рамках РЗПД, соблюдение законодательства, открытость, честность от начала до конца в использовании персональных данных);

конкретные цели (все конкретные цели и задачи должны быть закреплены в политике конфиденциальности и четко соблюдаться);

минимизация использованных данных (использование адекватного количества данных для выполнения поставленных целей, ограничение только необходимым количеством данных);

точность (персональные данные должны быть точными, не должны вводить в заблуждение; неправильные (несоответствующие) данные подлежат исправлению);

ограничение срока хранения данных (данные не следует хранить дольше, чем нужно для решения задач их сбора и обработки, необходимо периодически проводить аудит данных и удалять неиспользуемые);

целостность и конфиденциальность/безопасность (хранение данных в безопасном месте и в безопасных условиях (с соблюдением режима безопасности), необходимость уделять достаточное внимание сохранности данных);

подотчетность (ответственность за обработку персональных данных и выполнение всех остальных принципов РЗПД, включая наличие отметок о соблюдении положений о конфиденциальности; защите, использовании, проверке данных; назначении должностного лица по защите данных (англ.: data protection officer, DPO).

РЗПД регулирует действия и контролера данных (Data controller – организация, собирающая данные), и обработчика данных (Data processor – организация, которая обрабатывает данные от имени контролера данных, например, поставщик облачных услуг). Контролер данных определяет цель и задачи обработки персональных данных, а обработчик ответственен за непосредственную обработку данных, но оба несут ответственность за соблюдение норм РЗПД.

В отличие от Директивы ЕС 95/46, постановление 679/2016 не требует от государств-участников разработки национальных подходов к регулированию защиты физических лиц при обработке персональных данных, поскольку вопрос в полной мере урегулирован в рамках РЗПД, и положения Регламента являются непосредственно обязательными к исполнению (они должны были быть имплементированы в национальные регулирующие правовые акты до 25 мая 2018 г.: в качестве примера законодательного акта, в который, в связи с принятием РЗПД, имплементированы положения Регламента, можно привести датский Закон о дополнительных мерах по регулированию защиты физических лиц при обработке персональных данных и о свободном обращении таких данных [24]). Это применимо не только к резидентам государств-участников, но также к любому юридическому лицу, обрабатывающему персональные данные резидентов ЕС.

За невыполнение Регламента может быть наложен штраф до 20 млн евро или до 4% годового мирового оборота компании за предыдущий финансовый год (в зависимости от того, какая сумма больше).

В Регламенте расширено понятие персональных данных, введены понятия «трансграничной передачи данных», «псевдонимизации», установлено «право на забвение», определена роль должностного лица по защите данных.

Далее рассмотрены некоторые положения РЗПД, в большей мере относящиеся к ДСЗ.

В пункте 35 преамбулы РЗПД определено, что персональные данные, касающиеся здоровья, должны включать все данные, относящиеся к состоянию здоровья субъекта данных, которые содержат/будут содержать информацию об его/ее физическом или психическом здоровье в прошлом, в настоящее время и в будущем. Это включает в себя информацию о физическом лице, полученную при его/ее регистрации в качестве пациента; номер, символ или идентифицирующий символ, присвоенный физическому лицу, позволяющие его/ее однозначно идентифицировать как получателя медицинской помощи; данные обследований и исследований, включая генетическую информа-

цию и биологические образцы; любую иную информацию о, например, заболевании, инвалидности, риске заболевания, истории болезни, лечении, физиологическом, биомедицинском состоянии субъекта данных, вне зависимости от источника получения этой информации, например, от врача или иного медицинского работника, из организации здравоохранения, непосредственно в ходе инструментальных и лабораторных (in vitro) диагностических исследований.

При этом, конкретное определение персональных данных, касающихся здоровья, содержится в пункте 15 статьи 4 РЗПД: ДСЗ – персональные данные относительно физического или психического здоровья физического лица, включая оказание ему/ей медицинских услуг, в ходе которого получается дополнительная информация о состоянии здоровья пациента.

Определены конкретные основания для отступления от запрета обработки ДСЗ (пункт 52 преамбулы):

если обработка этих данных предусмотрена в законодательстве ЕС или государстве-члене ЕС и обеспечивается надлежащими гарантиями, такими как защита персональных данных и других фундаментальных прав и свобод человека;

если обработка этих данных представляет общественный интерес, в частности, обработка ДСЗ при приеме на работу (определенные требования к работнику со стороны работодателя), при начислении и выплате пенсий (заинтересованные – органы и организации социальной защиты), для обеспечения безопасности в сфере здравоохранения, в целях мониторинга и оповещения, профилактики или контроля инфекционных заболеваний и других серьезных угроз здоровью;

обработка ДСЗ в целях здравоохранения, включая организацию здравоохранения и управление отраслью, в частности, в целях обеспечения качества, доступности и эффективности оказания медицинской помощи, урегулирования претензий страховых медицинских организаций;

для достижения общественно важных научных, исторических, статистических целей;

при рассмотрении исковых заявлений, вне зависимости от того, происходит ли это в ходе судебных разбирательств или административной процедуры.

Указано, что РЗПД обеспечивает создание гармонизированных условий для обработки специальных персональных данных, касающихся здоровья человека, в конкретных обстоятельствах, в частности, когда обработка информации осуществляется для определенных целей, связанных со здоровьем человека, лицом, несущим правовые обязательства по сохранению врачебной тайны (пункт 53 преамбулы).

Обработка ДСЗ может быть необходима в общественно важных целях в сфере общественного здравоохранения и, вследствие этого, осуществлена без согласия субъекта данных (пункт 54 преамбулы). При этом, обязательно должны быть приняты надлежащие и конкретные меры по защите прав и свобод физических лиц. В данном контексте к сфере общественного здравоохранения отнесено решение всех вопросов, касающихся здоровья, определения состояния общественного здоровья, включая заболеваемость и инвалидность; исследования факторов, оказывающих влияние на состояние здоровья; определения потребностей здравоохранения; ресурсов, выделяемых на здравоохранение; обеспечения всеобщего доступа к услугам здравоохранения; определения расходов на здравоохранение; исследования причин смертности. Обработка ДСЗ в общественно важных целях здравоохранения не должна приводить к обработке информации в других целях третьей стороной (наниматели, страховые, банковские компании).

Согласно положениям пункта 63 преамбулы, субъект данных должен иметь право доступа к собственным ДСЗ, что включает доступ к информации, касающейся его здоровья, например, к информации из его медицинских документов (диагнозы, результаты медосмотра, оценка лечащими врачами эффективности любого вида осуществленного лечения или вмешательства), и использовать это право беспрепятственно и в разумных временных интервалах в целях ознакомления и верификации законности обработки данных.

Пункт 71 преамбулы содержит указание на то, что в отношении субъекта данных не должны приниматься решения, которые могут включать меры, оценивающие его личные качества на основании исключительно автоматической обработки его личных данных (подобная обработка включает профайлинг), что приводит к затрагивающим его/ее правовым последствиям или возможности принятия существенных для субъекта решений (автоматический отказ в выдаче онлайн-кредита; отказ в приеме на работу, если набор осуществляется через Интернет без какого-либо визуального контакта). Эти действия возможны только в том случае, если субъект данных выразил свое четкое согласие на это, а также, когда это предусмотрено законодательством ЕС или государства-члена ЕС, которому подчиняется контролер, для борьбы с мошенничеством и уклонением от уплаты налогов, обеспечения безопасности услуг, предоставляемых контролером, или в целях необходимости заключения договора между субъектом данных и контролером.

Определены принципы, применяемые при обработке персональных данных (статья 5):

1. Персональные данные должны быть:

a) обработаны законным, справедливым и прозрачным способом по отношению к субъекту данных («законность, справедливость и прозрачность»);

b) собраны в конкретных, четко выраженных и законных целях и не обрабатываться таким способом, который несовместим с этими целями; обработка информации в общественно важных, научных, исторических, статистических целях не должна быть несовместимой с изначальными целями;

c) адекватными, релевантными и собранными в объеме, который необходим в заявленных целях их обработки («минимизация информации»);

d) точными и, если необходимо, обновляемыми; любое разумное действие должно быть предпринято в целях обеспечения того, чтобы неточная, имеющая отношение к целям, ради которых она обрабатывается, информация была незамедлительно уничтожена или исправлена («точность»);

e) хранимыми в форме, которая позволяет обеспечить идентификацию субъекта информации, в течение срока, не превышающего необходимый в заявленных целях обработки данных; продление срока хранения данных возможно в том случае, если они обрабатываются исключительно в общественно важных научных, исторических, статистических целях при принятии соответствующих технических и организационных мер для соблюдения гарантий прав и свобод субъекта данных («ограничение на хранение информации»);

f) обработаны таким способом, который обеспечивает надлежащую безопасность персональных данных, включая защиту от неавторизованной и незаконной обработки и от случайной утери, уничтожения, с использованием при этом соответствующих технических и организационных мер («целостность и конфиденциальность»).

2. Контролер должен быть ответственен за соблюдение пункта 1 этой статьи и должен быть способен продемонстрировать свое выполнение этих требований («отчетность»).

В статье 6 РЗПД указаны случаи, когда обработка данных является законной.

Наиболее важные регулирующие положения по теме настоящего исследования приведены в статье 9 Регламента, пункт 1 которой содержит указание на то, что обработка персональных данных, в том числе касающихся здоровья человека, должна быть запрещена.

В пункте 2 статьи 9 перечислены все исключения из этого общего правила, а именно:

обработка ДСЗ возможна, если:

субъект данных предоставил свое согласие на обработку информации в одной или более конкретных целях, за исключением случаев, когда законодательство ЕС или государства-члена ЕС предусматривает, что запрет, указанный в пункте 1 статьи 9, не может быть снят субъектом данных;

обработка необходима в целях осуществления обязательств и осуществления специальных прав контролера или субъекта данных (прием на работу, общественная безопасность, социальная защита), если это соответствует законодательству ЕС или государства-члена при обеспечении соответствующих гарантий соблюдения фундаментальных прав и интересов субъекта данных;

обработка необходима в целях защиты существенных интересов субъекта данных или других физических лиц, когда субъект данных физически или согласно законодательству не способен предоставить подобное согласие;

обработка осуществляется фондом, ассоциацией или другой некоммерческой структурой в рамках законной деятельности, с соблюдением соответствующих гарантий, в указанных определенных собственных политических, философских, религиозных или профсоюзных целях, и при условии, что обработка затрагивает исключительно членов или бывших членов соответствующей структуры или лиц, которые имеют постоянный контакт с ними, и, при этом, персональные данные не раскрываются вне данной структуры (в этом случае обработка данных возможна без наличия согласия субъекта данных);

обработка касается персональных данных, которые явно были сделаны публично доступными субъектом данных;

обработка необходима для создания и защиты правовых требований, если соответствующие судебные инстанции действуют в пределах своей компетенции;

обработка необходима для реализации целей, представляющих существенный общественный интерес, при этом, она должна осуществляться в соответствии с законодательством ЕС или государства-члена ЕС, по объему быть пропорциональной преследуемым целям, должны приниматься надлежащие и конкретные меры по защите персональных данных и других фундаментальных прав и интересов субъекта данных;

обработка необходима в целях профилактической медицины, гигиены труда, медицинской экспертизы и реабилитации, диагностики, предоставления медико-социальной помощи, лечения, организации и управления здравоохранением, при этом, она должна осуществляться в соответствии

с законодательством ЕС или государства-члена ЕС, должны приниматься надлежащие и конкретные меры по защите персональных данных и других фундаментальных прав и интересов субъекта данных;

обработка необходима в общественно важных целях в сфере общественного здравоохранения, таких как защита от серьезных трансграничных угроз здоровью населения или обеспечение высоких стандартов качества и безопасности медицинской помощи, при этом, она должна осуществляться в соответствии с законодательством ЕС или государства-члена ЕС, которое предусматривает надлежащие и конкретные меры для защиты прав и свобод субъекта данных, в частности, соблюдение врачебной тайны;

обработка необходима в общественно важных научных, исторических, статистических целях, при этом, она должна осуществляться в соответствии с законодательством ЕС или государства-члена ЕС, по объему быть пропорциональной преследуемым целям, должны приниматься надлежащие и конкретные меры по защите персональных данных и других фундаментальных прав и интересов субъекта данных.

Статья 17 РЗПД содержит гарантии права субъекта данных на их уничтожение («право на забвение»), определены случаи, когда данные должны быть уничтожены в обязательном порядке.

15 декабря 1997 г. Европейским парламентом и Советом Европейского союза для содействия гармонизации положений законодательства государств – членов Европейского союза принята Директива №97/66/ЕС об использовании персональных данных и защите неприкосновенности частной жизни в сфере телекоммуникаций (далее – Директива 97/66/ЕС), которая перевела принципы, установленные в Директиве 95/46/ЕС в специальные правила, применяемые в сфере телекоммуникаций. Цель принятия данной Директивы – обеспечение эквивалентного уровня защиты основных прав и свобод человека, в частности права на невмешательство в частную жизнь при использовании персональных данных в секторе телекоммуникаций. Положения Директивы 97/66/ЕС применялись в отношении персональных данных, используемых в связи с оказанием общедоступных телекоммуникационных услуг посредством общедоступных телекоммуникационных сетей в рамках ЕС, а именно посредством цифровой сети интегрированных услуг и публичных цифровых мобильных сетей.

Директива 97/66/ЕС утратила силу в связи с принятием Директивы Европейского парламента и Совета Европейского союза 2002/58/ЕС в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи от 12 июля 2002 г. (далее – **Директива 2002/58/ЕС**) [25].

Директива 2002/58/ЕС обеспечивает гармонизацию национальных положений, необходимых для гарантии соответствующего уровня защиты основных прав и свобод, в том числе права на частную жизнь и конфиденциальность информации о частной жизни в связи с обработкой персональных данных в сфере электронных коммуникаций, и для свободного обращения подобных данных.

Данная Директива применяется в отношении обработки персональных данных в связи с предоставлением общедоступных услуг электронной связи в сетях связи коллективного доступа в ЕС, в том числе в сетях связи коллективного доступа, поддерживающих сбор данных и устройства идентификации (статья 3).

В статье 4 содержатся указания на то, что провайдер общедоступных услуг электронной связи должен предпринять необходимые технические и организационные меры для обеспечения безопасности предоставляемых услуг, которые должны гарантировать уровень безопасности, соответствующий имеющимся угрозам, а именно:

гарантировать, что доступ к персональным данным может быть предоставлен только уполномоченному персоналу в разрешенных законом целях;

защищать персональные данные, сохраненные или переданные, от случайного или незаконного уничтожения, случайной потери или изменения, несанкционированного или незаконного хранения, обработки, доступа или раскрытия;

гарантировать введение политики безопасности в отношении обработки персональных данных.

При наличии определенной угрозы повреждения системы безопасности сети, провайдер общедоступных услуг электронной связи должен информировать абонентов в отношении такой угрозы, а в случаях, когда угроза выходит за пределы средств защиты, доступных провайдеру, – о любых возможных средствах защиты, включая информацию о затратах на их приобретение.

При наличии вероятности того, что повреждение системы безопасности персональных данных неблагоприятным образом затронет персональные данные или информацию о частной жизни абонента или индивидуального пользователя, провайдер также должен без необоснованного промедления уведомить абонента или индивидуального пользователя о таком повреждении.

Уведомление абонента или индивида должно, как минимум, описывать характер повреж-

дения системы безопасности персональных данных, содержать указание на контактные пункты, где можно получить дополнительную информацию, и на меры, которые могут быть приняты для того, чтобы смягчить возможные неблагоприятные последствия от повреждения в системе безопасности персональных данных. Уведомление, обращенное к национальным компетентным органам власти, должно, кроме того, описывать последствия повреждения системы безопасности персональных данных, меры, предложенные и принятые провайдером в отношении адресата, само повреждение системы безопасности персональных данных.

В соответствии с пунктом 3 статьи 5 Директивы 2002/58/ЕС государства-участники должны гарантировать, что хранение информации или получение доступа к информации, уже сохраненной на терминальном оборудовании абонента или пользователя, допускается только при условии, что заинтересованный абонент или пользователь дали свое согласие, будучи обеспеченными точной и полной информацией, помимо прочего, о целях обработки информации.

Также должны быть обеспечены гарантии того, что:

абоненты перед включением их в справочник бесплатно проинформированы о цели (целях) печатного или электронного справочника абонентов, находящегося в свободном доступе или запрашиваемого через справочные службы, в которые могут быть включены их персональные данные, и о любых дальнейших возможностях использования данных, основанных на функциях поиска, встроенных в электронные версии справочника (пункт 1 статьи 12);

абонентам предоставлена возможность определять, включены ли их персональные данные в общедоступный справочник. Если персональные данные абонентов включены в общедоступный справочник, то абонентам должна быть предоставлена возможность определять, до какой степени эти данные имеют отношение к целям справочника, определенным поставщиком справочника, а также возможность проверять, вносить исправления в данные или отзывать такие данные. Отказ абонентов от включения их данных в общедоступный справочник абонентов, проверка персональных данных, внесение в них исправлений или отзыв персональных данных из справочника абонентов должны осуществляться бесплатно (пункт 2 статьи 12).

Возможно выдвижение требования о том, чтобы для любых целей общедоступного справочника, иных, чем поиск деталей контакта людей на базе их имени и необходимого минимального количества других идентификационных признаков, было запрошено дополнительное согласие абонентов (пункт 3 статьи 12).

Директива Европейского парламента и Совета Европейского союза **2002/22/ЕС** от 7 марта 2002 г. об универсальных услугах и правах пользователей в отношении сетей электронных коммуникаций и услуг (Директива об универсальных услугах) [26] содержит положения, регламентирующие вопросы обращения и защиты персональных данных при составлении телефонных справочников и иных баз данных в области электронных коммуникаций.

Так, подчеркнута необходимость обеспечения права абонентов на тайну частной жизни, учитывая включение/внесение информации личного характера (персональных данных) в телефонные справочники в печатном или электронном виде (пункты 11, 35 преамбулы), подключение услуги «определитель номера» и детализацию счета (пункт 39 преамбулы); содержатся требования к провайдерам общедоступных услуг связи и электронных сетей коммуникаций уважать фундаментальные права и свободы граждан, в том числе, право на неприкосновенность частной жизни (пункт 3 статьи 1), указывать в договоре на оказание услуг связи информации о том, предоставляется ли доступ к услугам экстренной связи и информация о местонахождении звонящего (абзац второй подпункта 1b статьи 20), получать согласие абонента на включение его персональных данных в телефонный справочник (пункт 1c статьи 20), включать в договор любую другую информацию, которая в этих целях может быть предоставлена соответствующими государственными органами, о способах защиты от угроз личной безопасности, частной жизни (в частности, в отношении персональных данных), связанных с предоставляемыми услугами (часть вторая пункта 1 статьи 20; подпункт 4b статьи 21) и т.д.

Заключение. Учитывая закрепленные международными правовыми актами основополагающие права человека, европейскую практику правового регулирования отношений, связанных с обращением специальных персональных данных, а также отсутствие сформулированных за весь предшествующий период применения ИКТ в здравоохранении каких-либо новых, характерных исключительно для «эры ЭЗ», отличных от существующих, прав человека, при создании в Республике Беларусь единого информационного пространства здравоохранения (электронного здравоохранения) в части формирования и ведения ИЭМК возника-

ют и требуют правового регулирования в процессе нормотворчества *проблемные вопросы обеспечения права на выбор услуг, обязательного информированного согласия на услугу, права на отказ от оказания услуги, права собственного доступа и контроля доступа иных лиц (в том числе, медицинских работников) к персональной информации в системе ЭЗ, соблюдения врачебной тайны при свободном обращении ДСЗ.*

Литература

1. *Лапицкий, В.А.* Электронное здравоохранение Беларуси: состояние и перспективы / В.А.Лапицкий, И.Э.Том // Информатика. – 2018. – Т.15, №4. – С.7–15.
2. Клятва Гиппократа [Электронный ресурс]. – Режим доступа: http://www.bibliotekar.ru/3-1-58-pravo-v-medicine/2.htm. – Дата доступа: 10.04.2019.
3. *Кобринский, Б.А.* Конфиденциальность и защита персональных медицинских данных в системе электронного здравоохранения [Электронный ресурс] / Б.А.Кобринский. – Режим доступа: http://federalbook.ru/files/FSZ/soderghanie/Tom%2015/XI/Kobrinskiy.pdf. – Дата доступа: 10.04.2019.
4. *Кристальный, Б.В.* Законодательная поддержка развития электронного здравоохранения в России и других странах СНГ / Б.В.Кристальный, М.Я.Натензон // Информационные ресурсы России. – 2007. – №3. – С.2–7.
5. *Абламейко, М.С.* Правовые вопросы развития электронного здравоохранения в Республике Беларусь / М.С.Абламейко, С.В.Абламейко // Проблемы управления. – 2014. – №4 (53). – С.33–39.
6. Recommendation CM/Rec (2019) 2 of the Committee of Ministers to member States on the protection of health-related data [Electronic resource]. – Mode of access: https://www.coe.int/en/web/cm/-/1342nd-meeting-of-the-ministers-deputies-27-march-2019-#43507320_43507202_True. – Date of access: 19.04.2019.
7. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No.108 [Electronic resource]. – Mode of access: https://rm.coe.int/1680078b37. – Date of access: 10.04.2019.
8. О здравоохранении [Электронный ресурс]: Закон Респ. Беларусь, 18 июня 1993 г., №2435-XII // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.
9. The Rights of Patients // A Declaration on the promotion of patients' rights in Europe / WHO Regional office for Europe; ICP/HLE 121. – Copenhagen, Denmark, 28 June 1994. – P.9–15. – Mode of access: http://www.who.int/genomics/public/eu_declaration1994.pdf. – Date of access: 10.04.2019.
10. Об утверждении Программы социально-экономического развития Республики Беларусь на 2016–2020 годы [Электронный ресурс]: Указ Президента Респ. Беларусь, 15 дек. 2016 г., №466 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.
11. Об утверждении Концепции развития электронного здравоохранения Республики Беларусь: приказ Министерства здравоохранения Респ. Беларусь, 20 марта 2018 г., №244.
12. О некоторых вопросах формирования интегрированных электронных медицинских карт в Республике Беларусь: приказ Министерства здравоохранения Респ. Беларусь, 25 мая 2018 г., №536.
13. Терминология по общественному здоровью и здравоохранению / ГУ РНПЦ МТ (организация-разработчик); авторы-разработчики: Е.Л.Богдан (председатель рабочей группы) [и др.]. – Минск, 2017. – С.33.
14. *Зингерман, Б.В.* Электронная медицинская карта и принципы ее организации / Б.В.Зингерман, Н.Е.Шкловский-Корди // Врач и информационные технологии. – 2013. – №2. – С.37–58.
15. *Зингерман, Б.В.* Персональная электронная медицинская карта – сервис, доступный уже сегодня / Б.В.Зингерман // Врач и информационные технологии. – 2010. – №3. – С.15–25.
16. Международный пакт о правах человека («Всеобщая декларация прав человека») [Электронный ресурс]: одобр. резолюцией 217 А (III) Третьей сессии Генеральной Ассамблеи ООН, 10 дек. 1948 г. // Организация Объединенных Наций. – Режим доступа: https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/045/84/IMG/NR004584.pdf?Open Element. – Дата доступа: 30.08.2019.
17. Конвенция о защите прав человека и основных свобод (Европейская конвенция по правам человека, измененная и дополненная Протоколами №11 и №14 в сопровождении Дополнительного протокола и Протоколов №4, 6, 7, 12 и 13) [Электронный ресурс]. – Страсбург: Европейский суд по правам человека. – 32 с. – Режим доступа: https://www.echr.coe.int/Documents/Convention_RUS.pdf. – Дата доступа: 30.08.2019.
18. Международный пакт о гражданских и политических правах [Электронный ресурс]: одобр. резолюцией 2200 А (XXI) Двадцать первой сессии Генеральной Ассамблеи ООН, 16 дек. 1966 г. // Организация Объединенных Наций. – Режим доступа: https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NL6/600/01/IMG/NL660001.pdf?Open Element. – Дата доступа: 30.08.2019.
19. Конституция Республики Беларусь: с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г. и 17 окт. 2004 г. – Минск: Нац. центр правовой информ. Респ. Беларусь, 2016. – 62 с.
20. Протокол к Конвенции 108 о наблюдательных органах и трансграничной передаче информации ETS 181 [Электронный ресурс]. – Режим доступа: https://pd.rkn.gov.ru/law/. – Дата доступа: 10.04.2019.
21. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing

of Personal Data No.223 [Electronic resource]. – Mode of access: https://rm.coe.int/16808ac918. – Date of access: 10.04.2019.
22. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Electronic resource]. – Mode of access: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046. – Date of access: 01.05.2019.
23. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Electronic resource]. – Mode of access: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. – Date of access: 01.05.2019.
24. Act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act) No.502 of 23 May 2018 [Electronic resource]. – Mode of access: https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf. – Date of access: 01.05.2019.
25. Директива Европейского парламента и Совета Европейского союза 2002/58/ЕС в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи от 12 июля 2002 г. (Директива о конфиденциальности и электронных средствах связи) (текст в редакции Директивы 2006/24/ЕС Европейского парламента и Совета ЕС от 15 марта 2006 г., Директивы 2009/136/ЕС Европейского парламента и Совета ЕС от 25 ноября 2009 г.) [Электронный ресурс]. – Режим доступа: https://zakon.rada.gov.ua/laws/show/994_b34. – Дата доступа: 01.05.2019.
26. Директива Европейского парламента и Совета Европейского союза 2002/22/ЕС от 7 марта 2002 г. об универсальных услугах и правах пользователей в отношении сетей электронных коммуникаций и услуг (Директива об универсальных услугах) (текст в редакции Директивы 2009/136/ЕС Европейского парламента и Совета ЕС от 25 ноября 2009 г.) [Электронный ресурс]. – Режим доступа: https://pd.rkn.gov.ru/law/. – Дата доступа: 01.05.2019.

HUMAN RIGHTS IN E-HEALTH ERA IN TERMS OF PHYSICIAN – PATIENT RELATIONSHIP. PART 1. EUROPEAN PRACTICE OF LEGAL REGULATION OF RELATIONS WITH REGARD TO SPECIAL PERSONAL DATA MOVEMENT

N.Ye.Kheifets, Ye.N.Kheifets

Republican Scientific and Practical Center for Medical Technologies, Informatization, Administration and Management of Health (RSPC MT), 7a, P.Brovki Str., 220013, Minsk, Republic of Belarus

Focus is identified of legal mechanism on patient rights' ensuring when introducing e-health. Basic international legal acts on protection of natural persons with regard to automatic processing of special personal data (and, in particular, special personal health-related data, HRD) and on the free movement of such data have been analyzed. Current world practice of legal regulation of issues of human rights ensuring when providing e-health services (right to choose services, mandatory prior informed consent to the service, right to refuse e-health services, right of own access and control of other persons' access (including medical professionals) to special personal data in e-health system, doctor – patient confidentiality protection on HRD free movement, etc.) has been studied to develop proposals on prevention violations of these rights through rulemaking process when introducing e-health in the Republic of Belarus.

Keywords: physician – patient relationship; e-health; special personal health-related data; human rights; right to privacy; doctor – patient confidentiality; legal regulation.

Сведения об авторах:

Хейфец Николай Ефимович; ГУ «Республиканский научно-практический центр медицинских технологий, информатизации, управления и экономики здравоохранения», зав. лабораторией основ стандартизации и оценки медицинских технологий; тел.: (+37529) 7789996; e-mail: nikolai.kheifets@gmail.com.

Хейфец Евгений Николаевич, магистр юридических наук; ГУ «Республиканский научно-практический центр медицинских технологий, информатизации, управления и экономики здравоохранения», лаборатория основ стандартизации и оценки медицинских технологий, научный сотрудник; тел.: (+37529) 5521274; e-mail: zhenn1990@rambler.ru.

Поступила 10.09.2019 г.