**УДК 004.056**

***Мамедова М.Г.***
Институт Информационных Технологий НАНА, Баку, Азербайджан
masuma.huseyn@iit.ab.az

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ МЕДИЦИНСКИХ ДАННЫХ В ЭЛЕКТРОННОЙ СРЕДЕ

*Исследованы вопросы защиты персональных данных в системе электронной медицины. Приведены подходы к обеспечению информационной безопасности данных о состоянии здоровья пациентов в мировой практике, выделены специфические особенности персональных медицинских данных и показаны потенциальные угрозы конфиденциальности и безопасности медицинской и врачебной тайн в медицинских информационных системах. Рассмотрена правовая основа защиты персональных данных в Азербайджане и обоснована целесообразность разработки в республике нормативно-методических документов, регулирующих информационную безопасность персональной медицинской информации.*

***Ключевые слова:*** *персональные медицинские данные, защита информации, безопасность, конфиденциальность, несанкционированный доступ, врачебная тайна, угрозы*.

## Введение

Информатизация практически всех сфер общественной жизни с каждым годом все интенсивнее проникает в сферу медицины. Новые концептуальные подходы к компьютеризации медицины, выраженные в персоноцентрированном подходе к медицинским записям и создании электронной медицинской карты (ЭМК) пациентов, определили направления модернизации здравоохранения, выраженные в разработке электронных аналогов медицинских документов, появлении возможности эффективного организованного доступа к любой совокупности медицинских записей и первичных результатов исследований пациента за счет отделения медицинских данных от их источника, переходе к электронному документообороту, интеграции данных о состоянии здоровья каждого человека в специализированных центрах обработки информации разного уровня. Уровень развития информационных технологий, определивший возможность реализации ЭМК-инфраструктуры, способствовал расширению:

а) доступности медицинских услуг вне зависимости от времени и пространства нахождения зарегистрированной медицинской информации;

б) технических возможностей по копированию, повторному использованию и распространению информации;

в) доступа к средствам массовых коммуникаций.

Новые возможности открылись для развития телемедицинских технологий, позволяющих проводить удаленные консультации, обследования, обработку первичной информации в специализированных центрах, сократив при этом время обследования и повысив точность диагностики.

Однако на фоне указанных положительных изменений современные эффективные средства интеграции и быстрой обработки персональных медицинских данных (ПМД) успешно используются злоумышленниками, создающими угрозу правам и законным интересам человека. Поэтому задача обеспечения информационной безопасности персональных данных в условиях электронной медицины (э-медицины) на сегодняшний день достаточно актуальна.

**Проблемы обеспечения конфиденциальности и безопасности медицинской информации в мировой практике**

Информация о человеке, всегда представляющая огромный интерес, в условиях развития информационного общества приобрела еще большую ценность. Необходимость обеспечения безопасности персональных данных, ставшая объективной реальностью современности, особую остроту имеет в медицине. Международная практика показывает, что уязвимость конфиденциальности и безопасности ПМД является основным препятствием на пути эффективного развития электронной медицины (e-health). Так, медицинские организации, имеющие доступ к самой закрытой личной информации о человеке, обязаны гарантировать конфиденциальность и безопасность всей врачебной информации. Любая персональная медицинская информация, вне зависимости от ее носителя, будучи конфиденциальной, должна надежно управляться как субъектом данных – пациентами, так и поставщиками профессиональной медицинской услуги – медицинским персоналом. Каждая сторона с правами доступа должна быть уверена, что данные, на которые они опираются, были введены уполномоченными лицами.

Типовая медицинская система (МИС), обеспечивающая создание в медицинском учреждении (МУ) единого информационного пространства, автоматизирует и оптимизирует организацию лечебно-диагностических процессов и других сторон жизнедеятельности организации – от документооборота и ресурсного учета до ведения электронной истории болезни, клинических записей о пациенте, интеграции с медицинским оборудованием, осуществляет информационную, интеллектуальную поддержку деятельности всех служб медицинского учреждения, а также принятия врачебных и управленческих решений. Будучи предназначена для поддержки деятельности медицинского учреждения, МИС отличается от других программных продуктов прежде всего тем, что в ней хранится и обрабатывается персональная и конфиденциальная информация. Юридически медицинские сведения о пациентах относятся к информации, составляющей врачебную тайну, доступ к которой ограничен и регламентируется действующим в каждой стране законодательством. В этой связи при разработке МИС обязательно должны быть учтены и реализованы ряд мер по обеспечению безопасности как информации, так и информационной системы в целом, в противном случае использование данной МИС неправомерно. Любой пользователь МУ, получающий доступ к МИС, несет полную (моральную, административную и уголовную) ответственность за обеспечение конфиденциальности информации, которую он вносит, использует или передает другим пользователям. Следовательно, обеспечение безопасности и конфиденциальности данных является одним из ключевых требований к современной МИС, и его реализация в информационно-коммуникационных и вычислительных системах является актуальной задачей [1–4].

Конфиденциальность ПМД выражена в том, что медицинские учреждения, получившие доступ к персональным данным, обязаны не раскрывать и не распространять персональные данные без согласия пациента. Законодательно это требование означает, что любой медицинский работник, получивший доступ к определенным ПМД, обязан хранить такую информацию и не передавать третьим лицам без согласия ее обладателя.

В контексте электронной медицины под безопасностью информации подразумеваются состояние защищенности индивидуально идентифицируемой медицинской информации, которая передается или поддерживается электронными медиа и любыми другими техническими средствами передачи и коммуникации, от внутренних или внешних угроз, а также защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования и блокирования.

Согласно мировой практике, информационная безопасность в системе э-медицины должна обеспечивать: 1) конфиденциальность (соблюдение врачебной тайны и защиту персональных данных), т.е. защиту от несанкционированного получения информации неавторизованными пользователями; 2) целостность, сводящуюся к гарантии достоверности и полноты информации при обмене данными и защите от несанкционированного изменения информации; 3) доступность, определяемую возможностью доступа авторизованных пользователей к информации и связанным с ней активам по мере необходимости, а также наличием режима отказоустойчивости МИС при взломе системы или ее перегрузке запросами [5–7].

Концепция персоноцентрированного подхода, являющегося главным трендом модернизации здравоохранения в странах ЕС, США, Канады, Австралии и др., базируется на принципе «чем проще доступ к медицинской информации, тем лучше медицинское обслуживание». Этот принцип, с одной стороны, предполагает упрощение доступа к персональной медицинской информации пациента (больного) для предоставления последнему оперативной квалифицированной медицинской помощи, а с другой – выдвигает серьезные требования к режиму информационной безопасности в этих странах, которая обеспечивается законодательно регулируемыми стандартами. Так, согласно Европейской директиве о защите данных (EU Data Protection Directive (1995) в странах – членах ЕС обеспечена гармонизация законодательства на уровне единого европейского пространства, и сегодня многие лечебные учреждения вправе иметь доступ к личным медицинским данным больного [8]. Опыт обеспечения режима информационной безопасности (ИБ) в информационных системах, включая и МИС, положен Международной организацией по стандартизации в основу стандарта ISO 27001, принятого также и в Азербайджане [9]. Режим информационной безопасности обеспечивается: 1) на организационном (административном и процедурном) уровне – политикой безопасности организации, в которой сформулированы цели и способы ее достижения; на процедурном уровне – путем разработки и выполнения инструкций по ИБ для персонала, а также мерами физической защиты; 2) на техническом (аппаратно-программном) уровне – применением апробированных и сертифицированных решений, стандартного набора контрмер: резервного копирования, антивирусной и парольной защиты, межсетевых экранов, шифрования данных и т.д.

Для идентификации отправителя (автора) электронного документа и гарантии неизменности его содержания (отсутствия искажений информации) используется электронная подпись, которая в случае внесения изменений в электронном документе теряет силу. В отношении коррекции данных, в отличие от их просмотра, требования еще более строгие, а изменения после завершения сеанса работы с ЭМК пациента исключаются. В противном случае при внесении исправлений в ранее созданный и подписанный средствами электронной подписи текст предшествующие записи должны сохраняться, оставаясь недоступными медицинским работникам подразделений при просмотре ЭМК, то есть реализуется механизм подотчетности, именуемый протоколированием действий и аудитом [5–9].

Закон о преемственности и подотчетности медицинского страхования (Health Insurance Portability and Accountability Act – HIPAA), принятый в 1996 году, представляет собой федеральный закон США, определяющий правила конфиденциального и безопасного обмена личной медицинской информацией и ее защиты от неразрешенного использования. Закон распространяется на персональную медицинскую информацию, хранящуюся как на бумажных носителях, так и в электронном виде [10].

Закон HIPAA основывается на двух важных идеях в осуществлении ухода за пациентом: неприкосновенность частной жизни и конфиденциальность. К неприкосновенности частной жизни относится право пациента на: а) ограничение того,

кто и что должен знать о его медицинском состоянии; 2) получение информации о том, кто имеет доступ к его данным и с какой целью (принцип прозрачности).

**Специфические особенности персональных медицинских данных**

При разработке системы безопасности ПМД и выборе оптимального режима информационной безопасности МИС наряду с необходимостью учета условий и угроз нарушения характеристик безопасности следует принять во внимание специфику, состав, а также участников обработки информации о пациенте. Под пациентом в данном случае подразумевается лицо, обращающееся к врачу для консультативной помощи и коррекции самочувствия, а больной – это пациент, заведомо нуждающийся в профессиональной лечебно-диагностической помощи. Как следует из приведенных определений, понятие "пациент" охватывает и понятие "больной".

Анализ литературных источников [11–14] дает возможность выделить следующие специфические особенности ПМД пациента:

1. Персональные медицинские данные пациента представляют собой закрытую личную (конфиденциальную) информацию о нем, причем правообладателем и распорядителем этих данных является последний, а не медицинское учреждение или медицинский работник. Это обуславливает особую форму отношений между пациентами как субъектами данных и пользователями их личной информации. Таким образом, одновременно необходимо защищать персональные данные и интересы частной жизни субъекта данных, врачебную тайну, ответственность и интересы профессионалов-медиков, законные интересы исследователей и других третьих лиц. При этом ряд персональных медицинских данных могут составлять врачебную тайну, в содержание которой включаются не только сведения медицинского характера, но и любые другие, которые были получены врачом в результате общения с пациентом.

2. Жесткий временной регламент на работу с медицинскими документами, вызванный необходимостью своевременного оказания медицинской помощи. Ухудшение данного показателя по причине усиления режима конфиденциальности информации в ущерб доступности данных для врачей может создать угрозу здоровью, а иногда и жизни больного. Поэтому необходимо обеспечить разумный компромисс между тремя составляющими обеспечения ИБ: конфиденциальностью, целостностью и доступностью данных.

3. ПМД пациента распределены по различным медицинским учреждениям, что позволяет фрагментировать последние: а) по анкетным данным, позволяющим однозначно идентифицировать пациента; б) по типу и характеру медицинских данных (информация о диагнозе, состоянии здоровья, рекомендации и назначения, информация о проведенном лечении, результаты лабораторных анализов, статистические данные и т.п.); в) по месту хранения (регистратура, родильный дом, УЗИ, лаборатория и т.п.), носителю информации (бумага, видео, электронные файлы) и автору отдельной медицинской информации (врачи и лечебные учреждения разного профиля, медсестра, лаборант и пр.).

4. Персональные медицинские сведения пациентов, полученные в различных географически и функционально удаленных МУ, как правило, не хранятся в одном месте. Это означает, что информация о медицинских услугах, оказанных в одном МУ, не доступна автоматически в другом МУ. Конфиденциальную информацию составляет только объединение всех или большинства распределенных фрагментов данных, и отдельные разделы медицинских данных тайны не представляют. Поэтому для обеспечения ИБ целесообразно организовать управление ограничением доступа с учетом многоуровневых ролевых обязанностей, полномочий и приоритетов медицинских специалистов и предоставить им в соответствии с функциональным назначением и при условии идентификации доступ к той или иной части информации [15, 16]. В настоящее

время этот подход, используемый в МИС развитых стран, каждому пользователю в соответствии с его полномочиями предоставляет доступ к определенным фрагментам ЭМК.

**Потенциальные угрозы конфиденциальности и безопасности персональных данных в МИС**

Согласно [11, 14, 17–19] при работе с персональными медицинскими данными могут возникнуть различные угрозы информационной безопасности. Прежде всего это угрозы конфиденциальности и безопасности информации, которые можно разделить на две основные категории:

I. Организационные угрозы, которые возникают из-за несанкционированного доступа к данным пациента со стороны: а) инсайдера – работника медучреждения; б) аутсайдера, эксплуатирующего систему, или хакера; в) уязвимости медицинских информационных систем. Организационные угрозы могут принимать различные формы. Широкий спектр организационных угроз можно разделить на пять уровней в порядке возрастания их сложности:

1. Случайное раскрытие личной информации: медицинский персонал непреднамеренно может разгласить информацию о пациенте другим, например, посредством e-mail или SMS сообщения, отправленного на ошибочный адрес или просочившихся в сеть сведений при обмене файлами.

2. Любопытство инсайдера: работник МУ с привилегиями доступа к ПМД пациента из любопытства или же целенаправленно может выйти, например, к информации о коллеге для выявления настоящей причины скрываемой последним болезни, приобретения персональных данных знаменитостей для распространения в средствах массовой информации и др.

3. Нарушение конфиденциальности ПМД со стороны инсайдера: медицинский персонал, имеющий прямой доступ к ПМД пациентов, сознательно использует (крадет) эту информацию для продажи и получения прибыли, а в некоторых случаях для нанесения морального и материального ущерба пациентам, коллегам и другим лицам. В разряд наиболее распространенных утечек относится предоставление за значительное вознаграждение фармацевтическим компаниям списков пациентов.

4. Нарушение неприкосновенности ПМД внешним агентом путем физического вторжения в помещение, в котором размещена информационная система ПМД: как правило, это злоумышленник (хакер), проникающий в информационную инфраструктуру организации для кражи данных или преднамеренного выведения ее из строя.

5. Несанкционированный доступ в сетевую инфраструктуру МИС: аутсайдеры (это могут быть бывшие сотрудники, пациенты, хакеры и т.п.), проникающие в сетевую систему организации извне с целью получения доступа к информации пациента или приведения системы в неработоспособное состояние, чаще с целью самоутверждения.

По состоянию на сегодня [20] наибольшую угрозу конфиденциальности и безопасности информации представляют внутренние нарушители – инсайдеры. Ведь злоумышленником может быть любой сотрудник медицинского учреждения – от рядовой медсестры до руководителя высшего ранга.

II. Технические (системные и физические) угрозы, которые возникают из-за нарушений в цепи потока информации вследствие неправомерного или случайного доступа к базе данных, несанкционированного искажения, уничтожения информации, разрушения физических носителей, сбоев в работе оборудования, возникающих при удалении файлов или поврежденных данных, а также непредвиденные последствия удаленного резервного копирования, несанкционированная модификация (подделка) данных и т.п.

Поскольку понятие ИБ персонифицировано в каждой конкретной ситуации, т.е. учитывает специфику объекта приложения, то для формирования технической составляющей системы защиты персональных данных в медицинских учреждениях разрабатываются руководящие и методические документы, определяющие состав общих и частных угроз типовой МИС, а также соответствующие меры защиты информации при обработке ПМД.

Международная практика показывает, что самая большая угроза для частной жизни в инфраструктуре электронных медицинских карт связана со вторичным использованием ПМД. Это касается тех случаев, когда информация, раскрываемая для определенной цели, впоследствии без авторизации субъекта данных может использоваться для других целей [14].

В настоящее время медицинские организации генерируют и хранят колоссальные массивы данных. Превратить эти «большие данные» (Big Data) в важнейшую практическую информацию является достаточно сложной задачей. А ведь обработка этой неструктурированной информации могла бы дать возможность получить уникальные знания [17]. Так, информация о ПМД пациентов играет важную роль в проведении клинических, эпидемиологических, экологических и других научных исследований, позволяющих разработать новые методы лечения различных болезней, собрать и проанализировать статистику, проверить фармакологическое воздействие новых лекарственных препаратов, улучшить качество здравоохранения, предсказания потенциально возможных вспышек различных заболеваний и т.п. Тем не менее, раскрытие информации о состоянии здоровья для исследователей вызывает озабоченность относительно нарушения конфиденциальности. Правила, определенные в нормативно-правовых актах, таких как HIPAA (США), позволяют медицинским организациям раскрывать медицинскую информацию для исследователей только в том случае, если они получили на это согласие от пациентов, или в исключительных случаях, предусмотренных законодательством. При этом обязательным условием для использования медицинской информации является обезличивание персональных данных.

В Регламент доступа к информации о состоянии здоровья включены государственные и частные медицинские учреждения, страховые компании, администраторы, врачи, аптеки, работодатели, учебные заведения, научные учреждения, дата-центры, организации по аккредитации и стандартизации, лаборатории, фармацевтические компании, финансовые агенты и т.п. К другой группе третьих лиц, заинтересованных в получении информации о пациенте, относятся родственники, работники здравоохранения, маркетологи, представители различных общественных программ содействия, кредитные бюро и правоохранительные органы.

Как следует из приведенного выше списка, в приобретении обезличенных медицинских данных пациентов заинтересован достаточно широкий круг лиц. Однако при всех благих намерениях относительно дальнейшего использования обезличенных ПМД пациентов существует вероятность злоупотребления этой информацией. Более того, наличие в Интернете открытой информации из социальных сетей, геолокационных сервисов, данных, полученных от фармацевтических компаний и других источников, позволяет выявить материальное состояние человека, его склонности, возможные заболевания и пр. Фармацевтические компании и страховые агентства, приобретая такую информацию, могут манипулировать ею. Кроме этого теоретически существует угроза «деанонимизации» электронной медицинской карты посредством сопоставления данных из разных источников.

Не случайно за последние годы продажа медицинской информации оформилась в отдельный сегмент «черного» рынка, а продажи конфиденциальной информации считаются одними из самых уязвимых и «высокодоходных». Ежегодно в развитых

странах из медицинских дата-центров «утекают» миллионы записей с персональными данными пациентов, а клиники теряют на этом миллиарды долларов. И чем масштабнее и глубже внедряются в отрасль электронные информационные системы, тем мощнее становится поток нелегитимного контента. Так, статистические данные по американскому рынку здравоохранения показывают [21], что самым распространенным источником утечек является кража, из-за которой происходят 45,2% случаев потери данных, причем в большинстве случаев материально заинтересованными медицинскими работниками разного ранга, имеющими прямой доступ к информации. Далее 22,1% случаев происходят в результате неавторизованного доступа к информации, 9,5% – связаны с потерями носителей информации, 6,1% – в результате хакерской атаки, 4,0% – из-за отсутствия пароля на электронном устройстве.

В качестве основных направлений возможных нарушений ИБ персональных медицинских данных можно выделить:

1) утечку и хищение данных, т.е. нарушение конфиденциальности (полное – при получении злоумышленником доступа к БД или частичное – при получении злоумышленником доступа к неразрешенной для него информации);

2) утрату данных вследствие разрушения носителей, несанкционированного уничтожения информации, стирания при непосредственном доступе к данным или посредством системы; утрата ПМД (информации о реакции на лекарства, аллергиях, перенесенных заболеваниях, результатах лабораторных анализов, терапии и пр.) может способствовать потере времени для их восстановления и, соответственно, спасения жизни человека;

3) случайное, преднамеренное искажение или несанкционированная модификация (подделка) данных посредством системы или при непосредственном доступе к БД приводит к ошибочности медицинской информации, что, в свою очередь, обуславливает принятие неверных врачебных решений и назначений, представляющих опасность для жизни и здоровья человека.

Нарушения информационной безопасности ПМД могут иметь достаточно серьезные моральные, физические и материальные последствия, затрагивающие: 1) неприкосновенность частной жизни; 2) личное здоровье и безопасность; 3) финансовую и коммерческую конфиденциальность; 4) неоправданную дискриминацию со стороны работодателей, страховых компаний; 5) препятствия для политического и карьерного роста и пр.

Информационная безопасность ПМД в условиях электронной медицины обеспечивается за счет взаимоувязанного комплексного использования соответствующей правовой базы, организационных мер, программных и технических средств защиты. При этом следует также обратить внимание на морально-этические аспекты разглашения ПМД и законодательно закрепленную ответственность за нарушение конфиденциальности и нанесенный гражданину вред [22]. Рисунок 1 демонстрирует классификацию мер защиты персональных медицинских данных.

Хотя в различных нормативных документах развитых стран (США, Канада, Австралия, страны ЕС) и закреплена ответственность операторов дата-центров за распространение личных данных и предусмотрены наказания в виде довольно внушительных штрафов, однако пока эти меры не защищают от утечек конфиденциальной информации. Нарастание волны утечек эксперты объясняют как минимум двумя причинами – несовершенством медицинских информационных систем и слабостью законодательной базы [21, 23, 24].


Рис.1. Классификация мер защиты персональных медицинских данных

**Правовая основа защиты персональных медицинских данных в Азербайджане**

За последние два десятилетия процессам информатизации в Азербайджане уделяется значительное внимание, страна достигла больших успехов в направлении создания информационного общества. Несмотря на это, следует отметить, что по уровню цифровизации здравоохранение остается одной из наименее информатизированных отраслей национальной экономики и развитие МИС в этой сфере находится пока в начальной стадии [25–27].

Тем не менее проблемы хранения и передачи медицинских данных в электронном виде, защиты данных пациентов на электронных носителях в государственных структурах и в частной медицине, обеспечения конфиденциальности медицинской информации о пациентах и деятельности самого медицинского учреждения и др. находятся в центре внимания как уполномоченных органов, так и исследователей и разработчиков.

В настоящее время информационная безопасность персональных медицинских данных в Азербайджане регулируется в основном следующими политическими документами:

1. Всеобщая декларация прав человека, Организация Объединенных Наций (ООН), 10 декабря 1948 г.

2. Конвенция Совета Европы "О защите личности в связи с автоматической обработкой персональных данных", 28 января 1981 г.

3. Конституция Азербайджанской Республики, 3 августа 2003 г.

4. Закон Азербайджанской Республики "О персональных данных", 11 мая 2010 г.

5. Закон Азербайджанской Республики об охране здоровья населения, 25 июня 1997 г.

6. Закон Азербайджанской Республики "Об информации, информатизации и защите информации", 3 апреля 1998 г.

7. Закон Азербайджанской Республики "Об электронной подписи и электронном документе", 9 марта 2004 г.

В соответствии со статьей 12 Всеобщей декларации прав человека [28] «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".

Учитывая важность и ценность информации о человеке, а также заботясь о соблюдении прав своих граждан, государства различных стран требуют от организаций и физических лиц обеспечения надежной защиты персональных данных. Так, с этой целью в 1981 году Советом Европы была принята конвенция "О защите личности в связи с автоматической обработкой персональных данных" [29], ратифицированная странами – членами Совета Европы и открытая для принятия любой другой страной, не имеющей членства в СЕ. Данная конвенция, ратифицированная в 2009 году Милли меджлисом (парламентом) Азербайджана, вступила в силу в сентябре 2010 года, возложив на Азербайджанскую Республику обязательства по приведению в соответствие с нормами европейского законодательства деятельности в области защиты прав субъектов персональных данных. В направлении реализации взятых обязательств в мае 2010 года в республике принят закон "О персональных данных" [30], регулирующий отношения, связанные со сбором, обработкой и защитой персональных данных, формирования баз персональных данных в национальном информационном пространстве, а также вопросы, связанные с трансграничной передачей персональных данных, устанавливающие права и обязанности действующих в данной сфере государственных органов и органов местного самоуправления, физических и юридических лиц.

В соответствии со статьей 32 ("Право на неприкосновенность") Конституции Азербайджанской Республики [31] каждый обладает правом на неприкосновенность личной и семейной жизни и на защиту от незаконного вмешательства в личную и семейную жизнь, а статья 41 ("Право на охрану здоровья") декларирует недопустимость сокрытия со стороны должностных лиц информации, связанной с угрозой жизни и здоровью.

Защита конфиденциальной информации является одной из наиболее актуальных проблем, которую сегодня приходится решать в медицинском учреждении при цифровизации здравоохранения. Согласно закону Азербайджанской Республики "Об информации, информатизации и защите информации" конфиденциальной считается документированная информация, доступ к которой ограничивается в соответствии с законодательством Азербайджанской Республики и которая не подлежит передаче третьим лицам без согласия ее обладателя [32]. А использование электронной подписи в соответствии с законом Азербайджанской Республики "Об электронной подписи и электронном документе" [33] позволяет повысить конфиденциальность информационного обмена медицинскими данными, гарантирует достоверность содержания электронного документа, который теряет силу в случае внесения в него изменений.

В законе Азербайджанской Республики «О персональных данных» под персональными данными подразумевается любая информация, позволяющая прямо или косвенно определить личность человека. Этот закон обязывает все учреждения страны выполнять необходимые требования по организации обработки и защиты персональных данных. Естественно, закон «О персональных данных» распространяется и на

медицинские учреждения Азербайджанской Республики, в которых помимо общих персональных данных (ФИО, паспортные данные, адрес и т.д.) обрабатываются так называемые специальные категории персональных данных – сведения о состоянии здоровья пациентов, составляющие врачебную тайну.

Врачебная тайна является видом персональных данных, которые становятся известными медицинской организации при оказании медицинских услуг. Однако поскольку вопросы охраны здоровья и прав пациентов, в том числе и право на врачебную тайну, ее защиту и ответственность за разглашение, регулируются законом Азербайджанской Республики об охране здоровья населения [34], то интерпретация закона Азербайджанской Республики «О персональных данных» через призму персональных медицинских данных порождает определенные недоразумения и разногласия. Так, в соответствии с законом Азербайджанской Республики об охране здоровья населения сведения, составляющие врачебную тайну, одновременно подпадают под определение как "служебной" тайны, так и "персональных данных". Эти сведения, охватывающие факты, события и обстоятельства частной жизни, личную или семейную тайну, также позволяют идентифицировать личность гражданина.

Согласно статье 53 закона Азербайджанской Республики об охране здоровья населения врачебную тайну составляют: 1) информация о факте обращения гражданина за медицинской помощью; 2) диагноз его болезни; 3) состояние здоровья; 4) другие сведения, полученные во время обследования и лечения. Гражданину законодательно гарантируются содержание в тайне предоставленной им информации и ответственность за ее разглашение. В этой же статье декларировано, что с согласия гражданина или его законного представителя информация, составляющая врачебную тайну, может быть передана другим гражданам, должностным лицам в интересах обследования и лечения больного, для использования в проведении научных исследований, в публикациях в научной литературе, учебных и других целях. Однако в ряде случаев, противоречащих интересам общества и оговоренных в статье 53 закона, врач освобождается от обязательства соблюдения врачебной тайны. Так, врач обязан сообщать о выявленных им случаях инфекционных заболеваний и опасности их распространения, массового отравления, при подозрении на противоправные действия и нанесении вреда здоровью граждан и т.п.

В соответствии со статьей 52 закона Азербайджанской Республики об охране здоровья населения врачи, нарушившие "Клятву Гиппократа", отражающую на протяжении многих веков (с III века до н.э.) морально-этические аспекты врачебной деятельности, несут ответственность в законодательно установленном порядке.

**Новые реалии, определяющие целесообразность развития законодательной базы и концептуальных подходов в сфере защиты ПМД**

В настоящее время медицинская сфера в странах, являющихся членами СНГ, в том числе и в Азербайджане, находится в сфере действия общего законодательства в области ИБ персональных данных, направленных на обеспечение защиты прав и свобод граждан при обработке их данных, в том числе защиту прав на неприкосновенность частной жизни, личной и семейной тайны. Между тем эксперты заостряют внимание на специфике данной сферы, с учетом которой целесообразным представляется создание отдельной регуляторной базы по аналогии с таковыми в ряде отраслей (например в банковской сфере). Отсутствие нормативной базы, регламентирующей порядок защиты и обеспечения безопасности сведений, составляющих врачебную и медицинскую тайны, в странах СНГ зачастую обуславливают принятием неадекватных решений.

На практике возникает масса противоречивых ситуаций, законодательного разрешения которых на сегодня нет [35–37]. Так, например, вполне реальна угроза того, что уволившийся сотрудник МУ может унести с собой клиентскую базу. Однако в

действующем законодательстве защита ПМД от утечек информации не предусмотрена даже при наличии полного комплекта документов, регламентирующих обработку ПМД. Далее, большинство персональных данных пациентов, обрабатываемых в МИС, подпадает под "специальную категорию персональных данных" (сведения о состоянии здоровья, лабораторных исследованиях и пр.), а в ряде случаев и под категорию "биометрические персональные данные", что повышает требования к системе защиты [38]. Следует также учесть возможность осуществления медицинскими учреждениями безопасной трансграничной передачи персональных данных пациентов при телемедицине. Отсутствует и четкое представление в вопросах защиты личной тайны и персональных медицинских данных. Так, с одной стороны, информацию, отнесенную к этим видам тайн, надо защищать, с другой – некоторые данные обязательны к раскрытию (публикации). Согласно существующему законодательству субъектами сохранения врачебной тайны являются медицинские работники, и для обработки ПМД пациентов лицами, не являющимися медицинскими работниками и не обязанными хранить врачебную тайну, требуется согласие пациента в письменной форме. Но помимо медперсонала в МУ имеются также работники, выполняющие другие профессиональные функции. Например, функционирование любой МИС связано с администрированием, а администраторы (системные, баз данных, приложений и т.д.) медицинскими работниками не являются, хотя доступ к информации фактически имеют.

Следует отметить также стремительное внедрение Интернета вещей в медицине. Так, сегодня многие люди для отслеживания состояния здоровья, контроля питания, физических нагрузок и других жизненных показателей используют объединенные в сеть носимые устройства. Врачи имеют возможность оперативно и с высокой точностью настраивать и оптимизировать имплантируемые устройства, такие как кардиостимуляторы, причем часто – не прибегая к инвазивным вмешательствам [39]. Однако наряду с преимуществом внедрения сетевых технологий в медицине растут риски конфиденциальности информации о личности и здоровье пациента, поскольку в среде хакеров медицинские сведения считаются особенно ценными.

Международная практика показывает, что хотя существующие редакции нормативно-правовых документов в области персональных данных предоставляют достаточно гибкий инструмент для эффективной защиты последних от возможных угроз безопасности, однако необходима выработка дополнительных рекомендаций с шаблонами документов и моделью типовых угроз для типовой МИС среднестатистического (типового) МУ [40–42]. В США, Великобритании и ряде других стран существует отдельная законодательная база, регулирующая вопросы информационной безопасности персональных медицинских данных, в том числе врачебную и медицинскую тайны [9, 10, 43].

Таким образом, актуализируется необходимость разработки внутренних нормативных документов, регламентов, которые могли бы разъяснить работникам МУ, как действовать в условиях информатизации медицины. Далее, необходимо разработать модель типовых угроз, в соответствии с которыми должны быть выработаны меры по защите конфиденциальной информации, а также установлен уровень защищенности ПМД. При этом следует принять во внимание связь выбора уровня защищенности конкретной МИС с: 1) типом персональных данных; 2) количеством субъектов, сведения о которых хранятся в МИС; 3) статусом МУ (например, потенциальные типы угроз, актуальные в поликлинике управделами президента, в небольшом районном МУ могут не представлять опасности); 4) актуальностью угроз, зависящих от уязвимостей в системном ПО, прикладном ПО, и других типов (кража физических носителей, хакеры и т.п.). Именно с их учетом будут формироваться конкретная практика применения и типовые решения.

Учитывая мировой опыт в сфере создания специфических нормативно-правовых актов, регулирующих информационную безопасность персональной медицинской

информации, целесообразной представляется разработка уполномоченными органами, в том числе Министерством здравоохранения Азербайджана, нормативно-правовых и методических документов, регламентирующих особенности их реализации в медицинских учреждениях, взаимосвязь персональных данных и врачебной информации, порядок защиты и обеспечения безопасности сведений, составляющих врачебную и медицинскую тайны. Это позволит усилить внимание руководителей медучреждений, медицинского персонала и других заинтересованных сторон к проблеме защиты личной информации пациентов, хранящейся как на бумажных, так и электронных носителях информации.

В условиях развития электронной медицины, широкого внедрения компьютерных технологий обработки ПМД и трансграничного обмена последней, развития МИС требуется комплексный инновационный подход к разработке правовых, организационных и технологических гарантий защиты медицинской информации, в том числе составляющей врачебную тайну, от несанкционированного доступа. Для этого требуется учесть особенности реальной ситуации в области защиты ПМД. Так, в первую очередь, следует принять во внимание тот факт, что обеспечение информационной безопасности ПМД не разовое мероприятие, а непрерывный процесс [44]. Это означает, что систему информационной безопасности необходимо постоянно поддерживать в актуальном состоянии, учитывая при этом специфические особенности и динамичность МИС, возросшие технические возможности злоумышленников по копированию, перехвату и распространению информации, оперативное решение проблемы безопасной передачи данных, ресурсы, модель типовых угроз и уровень защиты ПМД конкретной организации и др. С другой стороны, реальная ситуация сегодня такова, что во многих МУ защите ПМД не уделяется должного внимания; выделяемых на защиту электронных баз ПМД пациентов средств недостаточно; не хватает, а чаще всего и отсутствует квалифицированный персонал, компетентный как в вопросах технической защиты информации, так и знакомый с соответствующим законодательством [36].

Одним из эффективных подходов в сложившейся ситуации может быть разработка систем поддержки принятия решений (СППР), позволяющих за счет накопления знаний высококвалифицированных экспертов-специалистов генерировать рекомендации по поддержке принятия уполномоченными лицами решений относительно информационной безопасности ПМД в МУ. СППР позволят идентифицировать и формализовать задачи принятия решений в процессе проектирования системы защиты ПМД, выявить и оценить потенциальные угрозы информационной безопасности каждого конкретного МУ, а также соответствующие мероприятия по защите ПМД, нейтрализации угроз и определению уровня обеспечения информационной безопасности, необходимого для ее нормального функционирования [45–47].

**Заключение**

Проведенное исследование позволило сделать следующие заключения:

1. В условиях развития электронной медицины, широкого внедрения компьютерных технологий обработки персональных медицинских данных и трансграничного обмена последними, развития медицинских информационных систем требуется комплексный инновационный подход к разработке правовых, организационных и технологических гарантий защиты медицинской информации, в том числе составляющей врачебную тайну, от несанкционированного доступа.

2. Проблема обеспечения защиты персональных данных в медицинских учреждениях имеет свою специфику, в соответствии с которой в странах с развитой электронной медициной разработана отдельная законодательная база, регулирующая вопросы информационной безопасности персональных медицинских данных, обеспечения конфиденциальности и неприкосновенности частной жизни, доступа к персональным

данным и ответственности за их использование.

3. Международный опыт в сфере защиты персональных медицинских данных актуализирует целесообразность разработки в Азербайджане нормативно-методических документов, регламентирующих действия, права и обязанности работников медицинских учреждений в условиях электронной медицины, порядок защиты и обеспечения безопасности сведений, составляющих врачебную и медицинскую тайны, информационную безопасность ПМД при обмене информацией как внутри страны, так и за ее пределами и т.п.

4. В условиях информатизации медицины целесообразна разработка новых концептуальных подходов к поддержке принятия уполномоченными лицами решений, направленных на обеспечение информационной безопасности персональных медицинских данных в медицинских учреждениях.

**Литература**


1. Chao H., Twu S., and Hsu C. A Patient-Identity Security Mechanism for Electronic Medical Records During Transit and At Rest, // Medical Informatics and the Internet in Medicine, vol.30, no.3, 2005, pp.227–240.
2. Абдуманонов А.А., Карабаев М.К. Алгоритмы и технологии обеспечения безопасности информации в медицинской информационной системе Externet // Программные продукты и системы, 2013, №1, с.150–155.
3. Wang J., Zhang Z., Yang X., Zuo L., Kim J. Data Security and Privacy of e-Healthcare in Electronic Medical Environment / Proc. of the 2nd International Conference on Sensor and its Applications, 2013, pp. 92–98.
4. Wilkowska W., Ziefle M. Privacy and data security in e-health: Requirements from the user's perspective. Aachen University, Communication Science, Germany/ Health Informatics Journal, 2012, vol.18, no.3, pp.191–201.
5. Кобринский Б.А. Конфиденциальность и защита персональных медицинских данных в системе электронного здравоохранения. Федеральный справочник. http://federalbook.ru/files/FSZ/soderghanie/Tom%2015/XI/Kobrinskiy
6. Ameen M. A., Liu J. W. and Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications // Journal of Medical System, 2012, vol.36, no.1, pp.93–101.
7. Baker D.B. Privacy and Security in Public Health: Maintaining the Delicate Balance between Personal Privacy and Population Safety / The 22nd Annual Computer Security Applications Conference, 2006, pp.3–22.
8. European Parliament and Council Directive 95/46/ EC of 24 October 1995 http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm
9. ISO 27001:2013 Information technology. Security techniques. Information Security management systems. Requirements.
10. Choi Y.B., Capitan K.E., Krause J.S., Streeper M.M/ Challenges Associated with Privacy in Healthcare Industry: Implementation of HIPAA and Security Rules. // Journal of Medical Systems, 2006, vol.30, no.1, pp.57–64.
11. Назаренко Г.И., Михеев А.Е., Горбунов П.А., Гулиев Я.И., Фохт И.А., Фохт О.А. Особенности решения проблем информационной безопасности в медицинских информационных системах, http://www.interin.ru/datas/documents/pib.pdf.
12. Agrawal R., Johnson C. Securing Electronic Health Records Without Impeding the Flow of Information // International Journal of Medical Informatics, 2007, vol.76, no.5-6, pp.471–479.
13. Gostin, L.O., Hodge, J.G. Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule // Minnesota Law Review, 2002, vol.86, pp.1439–1449.
14. Brands S. Privacy and Security in Electronic Health, www.credentica.com/ehealth.pdf

15. Gallaher M.P., O'Connor A.C., Kropp. B. The Economic Impact of Role-Based Access Control, National Institute of Standards and Technology Report, 2002.
16. Li N., Tripunitara M.V. Security Analysis in Role-Based Access Control. //ACM Transactions on Information and System Security, 2006, vol.9, no.4, pp.391–420.
17. Alyass A., Turcotte M., Meyre D. From big data analysis to personalized medicine for all: challenges and opportunities. BMC Medical Genomics 2015, www.biomedcentral.com/1755-8794/8/33
18. Appari A., Johnson M.E. Information Security and Privacy in Healthcare: Current State of Research. 2008. http://www.ists.dartmouth.edu/library/416.pdf .
19. Мамедова М. Проблемы информационной безопасности персональных данных в условиях электронной медицины. "İnformasiya təhlükəsizliyinin multidissiplinar problemləri" üzrə II respublika elmi-praktiki konfransının əsərləri, Bakı, 14 may, 2015, səh.52–55.
20. McAfee Labs. Threats Report – February 2015. www.mcafee.com/ru/security-awareness/articles/mcafee-labs-threats-report-q4-2014.aspx
21. Каныгина О., Журавлева Е., Сильва-Вега М. Мировая практика утечки информации http://vademec.ru/magazines/article31896.html
22. Laurinda B. Harman, Cathy A. Flite, Kesa Bond. Electronic Health Records: Privacy, Confidentiality, and Security.// AMA, Journal of Ethics, 2012, vol.14, no.9, pp.712–719. http://journalofethics.ama-assn.org/2012/09/stas1-1209.html
23. Защита информации от утечек (DLP-системы), www.zecurion.ru/
24. ФЗ-152 в здравоохранении: как "обезопасить" ЛПУ?, www.cnews.ru/reviews
25. Məmmədova M.H., Əliyev Ə.Q. E-səhiyyə sisteminin formalaşması və inkişaf etdirilməsi problemləri / "Elektron dövlət quruculuğu problemləri"I Respublika elmi-praktiki konfransının materialları, Bakı, 4 dekabr 2014, səh.160–162.
26. Səhiyyə Nazirliyinin əsasnaməsi, www.health.gov.az/sehiyye-nazirliyinin-esasnamesi.html
27. Elektron səhiyyə. http://e-sehiyye.gov.az
28. Всеобщая декларация прав человека. ООН, 10 декабря 1948 г. www.un.org/ru/documents/decl_conv/declarations/declhr.shtml
29. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. http://conventions.coe.int/Treaty/EN/Reports/Html/108.htm
30. Закон Азербайджанской Республики "О персональных данных". – Баку, 11 мая 2010 г. http://www.rabita.az/uploads/qanunverilcik/qanunlar_ru/opersonalnidannix.pdf
31. Конституция Азербайджанской Республики, Баку, 3 августа 2003 г. http://ru.president.az/azerbaijan/constitution/
32. Закон Азербайджанской Республики "Об информации, информатизации и защите информации" от 3апреля 1998 г. www.e-qanun.az
33. Закон Азербайджанской Республики "Об электронной подписи и электронном документе" от 9 марта 2004 г. www.e-qanun.az
34. Закон Азербайджанской Республики об охране здоровья населения, Баку, 25 июня 1997 г. www.sehiyye.gov.az
35. Защита врачебной тайны. К чему может привести информатизация медицины? http://www.aif.ru/society/healthcare/1158820
36. Столбов А. Обработка персональных данных в медицинских организациях // Врач и информационные технологии, 2007, №4, с.39–43.
37. Зиновьева О.В. Порядок предоставления сведений и ответственность за их разглашение. www.onegingroup.ru/
38. Imamverdiyev Y.N., Teoh A.B.J., Kim J. Biometric cryptosystem based on discretized fingerprint texture descriptors // Expert Systems with Applications, 2013, vol.40, no.4, pp.1888–1901.

39. Интернет вещей в сфере здравоохранения. Преимущества и риски. www.mcafee.com/ru/resources/reports/rp-healthcare-iot-rewards-risks-summary.pdf
40. Magnusson, R.S. The Changing Legal and Conceptual Shape of Health Care Privacy // Journal of Law, Medicine & Ethics, 2004, vol.32, no.4, pp.680–691.
41. De Vimercati SDC, Foresti S, Livraga G, Samarati P. Protecting privacy in data release / Aldini A., Gorrieri R. (eds) FOSAD VI. Berlin: Springer, 2011, pp.1–34.
42. Magnusson R.S. The Changing Legal and Conceptual Shape of Health Care Privacy// Journal of Law, Medicine & Ethics, 2004, vol.32, no.4, pp.680–691.
43. Hodge J.G., Gostin L.O., Jacobbson P.D. Legal Issues Concerning Health Information: Privacy, Quality, and Liability // Journal of American Medical Association, 1999, vol.282, no.15, pp.1466–1471.
44. Васильев В.И., Белков Н.В. Система поддержки принятия решений по обеспечению безопасности персональных данных // Вестник УГАТУ, 2001, т.15, №5 (45), стр.54–65.
45. Королева Н.А., Тютюнник В.М. Экспертная система поддержки принятия решений по обеспечению информационной безопасности организации. Тамбов, изд-во Нобелистика, 2006, 198 с.
46. Аббасов А.М., Мамедова М.Г. Методы организации баз знаний с нечеткой реляционной структурой. Баку, Элм, 1997, 256 с.
47. Eta S. Berner. Clinical decision support systems. Theory and practice. Springer Science+Business Media LLC, 2007, 278 p.

**UOT 004.056**

***Məmmədova Məsumə H.***
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
masuma.huseyn@iit.ab.az

**Elektron mühitdə fərdi tibbi məlumatların informasiya təhlükəsizliyi**

Elektron tibb sistemində fərdi məlumatların qorunması məsələləri tədqiq edilmişdir. Dünya praktikasında pasiyentlərin sağlamlıq vəziyyəti haqqında məlumatların təhlükəsizliyinin təmin edilməsinə yanaşmalar göstərilmiş, fərdi tibbi məlumatların spesifik xüsusiyyətləri qeyd edilmiş, informasiya sistemlərində tibbi və həkim sirlərinin məxfiliyi və təhlükəsizliyinə potensial təhdidilər araşdırılmışdır. Azərbaycanda fərdi məlumatların qorunmasının hüquqi əsasları nəzərdən keçirilmiş və respublikada fərdi tibbi məlumatların informasiya təhlükəsizliyini tənzimləyən normativ-metodiki sənədlərin işlənməsinin məqsədəuyğunluğu əsaslandırılmışdır.
***Açar sözlər:*** *fərdi tibbi məlumatlar, informasiyanın qorunması, təhlükəsizlik, məxfilik, icazəsiz giriş, həkim sirri, təhdidilər.*

***Masuma H. Mammadova***
Institute of Information Technology of ANAS, Baku, Azerbaijan
masuma.huseyn@iit.ab.az

**Information security of personal medical data in electronic environment**

Problems of personal data security in electronic medicine system are investigated. Approaches to support information security of health data of patients in the world practice are stated, specific features of the personal medical data are selected and potential threats of privacy and safety of medical secret in the medical information systems are shown. The legal base of personal data security in Azerbaijan has been considered, and feasibility of the development of normative and methodical documents regulating information security of personal medical data is justified in the republic.
***Keywords:*** *personal medical data, information security, safety, privacy, illegal access, medical secret, threats.*