Гайнуллина Элина Зульфатовна

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, egainullina99@mail.ru

Глущенко Екатерина Сергеевна

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, yekaterina_glushchenko@mail.ru

Руф Юлия Николаевна

кандидат экономических наук, доцент, доцент кафедры экономической безопасности, системного анализа и контроля Тюменского государственного университета, г. Тюмень, ruf2077@yandex.ru

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СФЕРЕ ЗДРАВООХРАНЕНИЯ

Аннотация. В современных условиях внедрения цифровых платформ, большой объём информации, в том числе и персональные данные, находятся в виртуальной форме и являются элементами электронного документооборота. В таких обстоятельствах повышается актуальность безопасности информации, которая находится в обороте. Авторами исследованы вопросы защиты персональных данных людей, при попадании в медицину, иными словами пациентов. По результатам исследования представлена оценка современного состояния системы безопасности в здравоохранении. Предложены методы и инструменты улучшения качества защиты хранения, обработки и передачи информации в медицинских учреждениях.

Ключевые слова: персональные данные, сфера здравоохранения, защита данных, информационная безопасность, врачебная тайна

Gainullina Elina Zulfatovna

Student of the specialty "Economic Security" at Tyumen State University, Tyumen, egainullina99@mail.ru

Glushchenko Ekaterina Sergeevna

Student of the specialty "Economic Security" at Tyumen State University, Tyumen, yekaterina_glushchenko@mail.ru

Ruf Yulia Nikolaevna

Candidate of Science (Economics), Associate Professor of the Department of Economic Security, System Analysis and Control at Tyumen State University, Tyumen, ruf2077@yandex.ru

ENSURING THE PROTECTION OF PERSONAL DATA IN THE FIELD OF HEALTHCARE

Abstract. In the modern conditions of the introduction of digital platforms, a large amount of information, including personal data, is in virtual form and is an element of electronic document management. In such circumstances, the security of the information that is in circulation increases. The authors investigated the issues of protection of personal data of people who get into medicine, in other words, patients. Based on the results of the study, an assessment of the current state of the security system in healthcare is presented. Methods and tools for improving the quality of protection of information storage, processing and transmission in medical institutions are proposed.

Keywords: personal data, healthcare, data protection, information security, medical confidentiality

В современных условиях развития цифровой экономики и компьютерного обеспечения довольно остро встает вопрос защиты информации, касающейся сферы здравоохранения в частности. На бытовом уровне это объясняется достаточно просто. Приобретая статус пациента, и обращаясь с определенной проблемой в специальные учреждения, а именно больницы и поликлиники, возникает потребность сохранения конфиденциальности данных.

На сегодняшний день одним из ведущих направлений в развитии медицины и института здравоохранения в целом, является активное внедрение компьютеризированных платформ и систем информационного обеспечения. Наиболее популярным примером такой тенденции является создание Единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ). Практическое значение данной систематизированной формы проявляется в сочетании технических и информационно-технологических средств. В совокупности они значительно облегчают процесс обеспечения информационной поддержки для осуществления деятельности участников системы здравоохранения. Использование данной информационной платформы способствует техническому развитию здравоохранения, повышению качества услуг в сфере организации охраны здоровья граждан, а также обеспечению открытости системы здравоохранения в общем. Не смотря на это, фактор открытости системы в совокупности с другими повышает актуальность вопроса о защите персональных данных участников ЕГИСЗ, а именно граждан, приобретающих статус пациента.

Общего рационального решения вопроса о защите персональных данных пациента нет. Причиной является отсутствие утвержденного единого подхода к безопасности информации в медицинских учреждениях. Следствием этого являются регулярно возникающие проблемы

утечки конфиденциальной информации. По данной причине лечебное учреждение вынуждено решать эту проблему самостоятельно. Личная информация, предоставляемая медицинским учреждениям со стороны пациента, напрямую является отражением его социального статуса, общего состояния здоровья, финансового благополучия и других аспектов жизни человека. Иными словами, пациент предоставляет комплекс взаимосвязанных данных. Соответственно, говоря о вопросе защиты данного комплекса, важна системность указанного подхода, который в свою очередь бы учитывал формирование локальных информационных систем. Эти системы рассчитаны как на работу одного медицинского учреждения, так и на объединение разрозненных элементов в единую региональную сеть с выходом на федеральный уровень.

Актуализация данной проблемы поддерживается государством и пути ее решения обсуждались в рамках программы XVIII Ассамблеи «Здоровая Москва», проходившей в январе 2021 года. На которой рассматривался вопрос технологии систематизации данных пациентов. В рамках круглого стола спикеры обсуждали текущий статус реализации проектов в сфере больших данных, делились кейсами, прогнозировали изменения, касающиеся перспектив развития технологии и сервисов для врачей и системы здравоохранения в сфере конфиденциальных данных большого объема. [1]

Процесс обработки персональных данных включает в себя действия, совершаемые с использованием или без использования средств автоматизации, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, блокирование, уничтожение информации.

Разглашение данных пациента, которые автоматически являются врачебной тайной запрещено, включая условия и сам факт наступления летального исхода для пациента. Медицинские учреждения обязаны хранить данные о здоровье каждого обратившегося человека в виде медицинской карты. На сегодняшний день этот процесс автоматизирован, т.е. медицинские карты представляют собой электронный файл, хранящийся в базе учреждения. Однако, проблема утечки информации может возникнуть на каждом этапе взаимодействия персонала медучреждения с персональными картами больных.

Обработка персональных данных пациентов состоит из нескольких этапов, а именно: сбор и запись сведений, систематизация полученных данных, хранение информации в базе, уточнение деталей и уничтожение неактуальной информации. К персональным данным относится любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Следует отметить, что вопрос об обеспечении безопасности и сохранности персональных данных на современном этапе развития российской медицины на законодательном уровне регламентирован достаточно строго.

В качестве нормативно-правового документа, в котором закреплено определение персональных данных, является Федеральный закон № 152 ФЗ «О персональных данных» от 27.07.2006 с учетом всех принятых позднее изменений и дополнений. Согласно данному закону, к персональным данным относится любая информация о физическом лице: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, идентификационные данные документов (паспорт, СНИЛС и т. п.), семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация. [2]

Несмотря на то, что в современном мире активно происходит процесс компьютеризации, при обработке персональных данных, так или иначе, участвует человек. Взаимодействие и всяческие операции с полученными данными регламентируются так же ФЗ № 152 от 27.07.2006, так, например, данный закон требует обеспечить защиту прав и свобод человека, обязует операторов обработки персональных данных обеспечить определенные уровни защищенности, установленные Постановлением Правительства РФ № 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Уровни являются требованиями, которые способны устранить определенные угрозы безопасности. Применяемые меры защиты не ограничиваются перечнем Постановления № 1119, более детально они отражаются в Приказе ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». [3]

В нормативно-правовых актах четко закрепляется и статус персональных данных. Согласно Федеральному закону № 149 от 27.07.2006 «Об информации, информационных технологиях и о защите информации», персональные данные определяются как информация ограниченного доступа или конфиденциальная информация. Условие секретности и требование не передавать такую информацию третьим лицам без согласия ее обладателя, является обязательным условием для выполнения лицом, получившим доступ к определенным данным [4]. В связи с этим, государство устанавливает определенные строгие правила и нормы для обработки такой информации.

В рамках здравоохранения персональные данные являются специализированной информацией, поскольку содержат сведения о состоянии здоровья пациента, о причинах обращения за медицинской помощью, диагноз и особенности лечения. Именно эти специальные сведения и объединяются под термином «врачебная тайна», сохранность которой регулируется Федеральным законом № 323 от 21.11.2011 «Об основах охраны здоровья граждан в Российской Федерации».

В рамках рассматриваемой темы стоит упомянуть о том, что Минздрав опубликовал Приказ № 911н от 24.12.2018 «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций».

На основании исследований Российской группы компаний InfoWatch, специализирующейся на информационной безопасности в корпоративном секторе, а именно защите корпораций от утечек информации и целевых атак извне, авторы приводят статистические данные. За 9 месяцев 2020 года в мире зарегистрировано на 7,4% меньше утечек, чем за аналогичный период прошлого года. В России за тот же период число утечек, наоборот, выросло на 5,6%. В глобальном распределении по отраслям на первом месте находится сектор высоких технологий с долей 21,9%, на втором банки и финансы, на долю которых приходится 18,9%, на третьем месте государственные органы – 16,2%, в данном рейтинге медицина занимает пятую позицию с долей в 9,9%. [5] Сегментация состоит из отраслей жизни, наиболее автоматизированных, в которых используется электронный документооборот (рисунок 1).

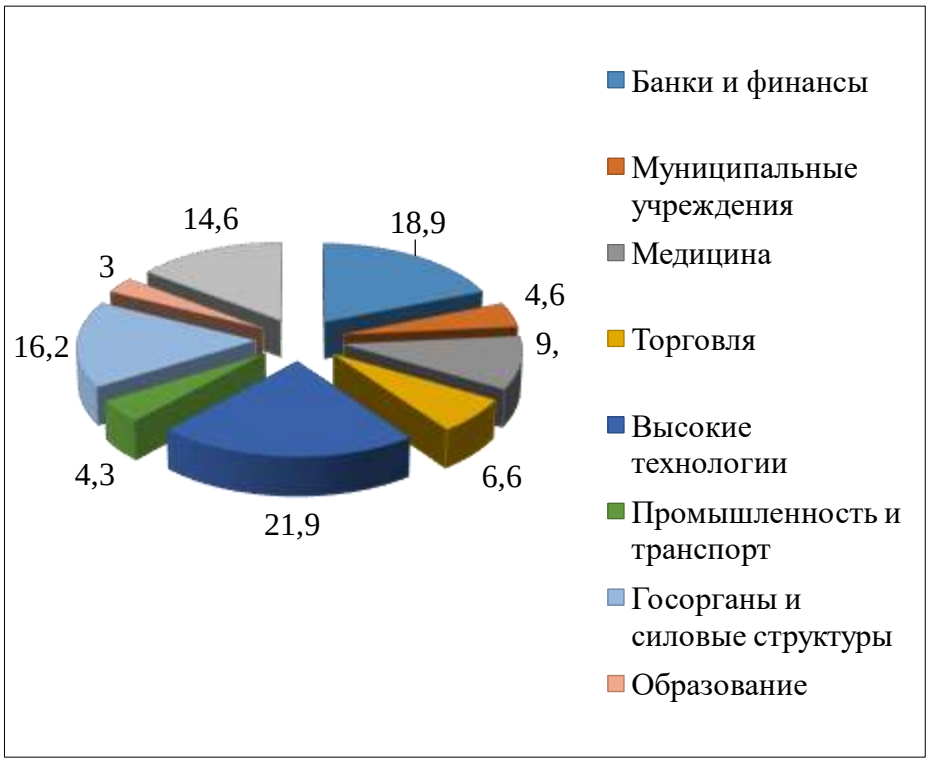

Рисунок 1. Отраслевое распределение информационных утечек по России с января по сентябрь 2020 г.

Источник: составлено авторами на основе данных [5]

Исходя из этого, здравоохранение можно отнести к лидерам по утечке данных. За 9 месяцев 2020 года такая проблема затронула две трети медицинских учреждений. Обработка информации в больницах, поликлиниках, стационарах и других медицинских учреждениях происходит посредством электронного документооборота или же ручного заполнения медицинскими работниками. В любом случае риск потери или утечки информации пропорционален ее объему. Информация может быть разного содержания, однако наиболее популярным видом, интересующим злоумышленников, являются именно персональные данные. Детальная сегментация представлена на рисунке 2.

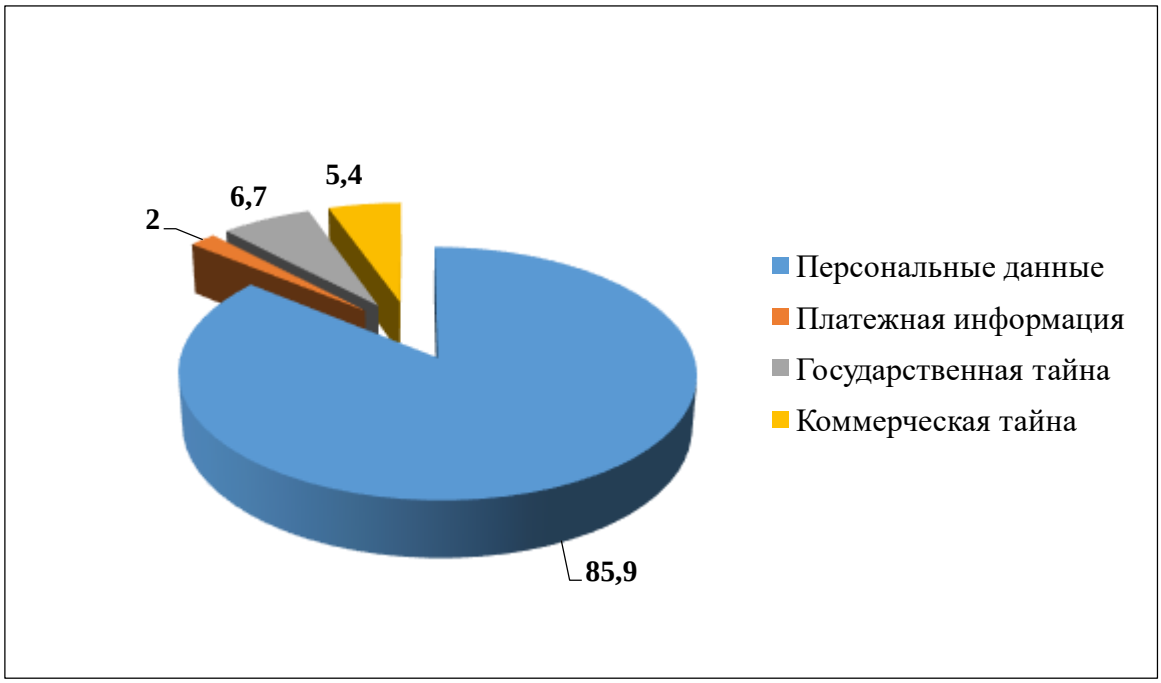

Рисунок 2. Распределение информационных утечек по типам данных по России с января по сентябрь 2020 г.

Источник: составлено авторами на основе данных [5]

Стоит так же взять во внимание, что не во всех медицинских организациях этот процесс автоматизирован, что повышает риск утечки или потери информации. Данные на бумажном носителе сильнее подвержены к утере, искажении и неправильности представленных данных. Неправильность представления данных чаще всего происходит посредством человеческого фактора, поскольку высокая загруженность становится причиной ошибок в заполнении документации. Практика показывает, что автоматизация в свою очередь не становится гарантом защищенности данных. Например, в медучреждениях, где уже установлены МИС или СЭД, данные могут пропадать из-за технических сбоев. Как упоминалось авторами ранее, человеческий фактор имеет место быть и в электронном документообороте. Это приводит к

риску некомпетентности и безответственному отношению лиц, отвечающих за безопасность данных пациентов.

Исходя из результатов исследования InfoWatch, около 80% проблем с защитой и безопасностью персональных данных возникает по вине штатных специалистов и происходит из-за халатности, а не по злому умыслу, а так же, почти 20% медицинских данных попадают в свободных доступ не в результате внешнего воздействия. [5]

На основании этих цифровых данных, авторами выделена еще одна причина – отсутствие качественной и отработанной коммуникации между медучреждениями и разработчиками программ электронного документооборота. Зачастую происходит конфликт интересов, поскольку разработчики предлагают информационные системы и программное обеспечение, не предполагающее защиту данных. Тем самым перенося решение вопроса на организации, которые не совсем компетентны в этом. Отсутствие необходимых компетенций превращается в безалаберное отношение к вопросу конфиденциальности данных со стороны сотрудников медицинских учреждений. Существование такого разногласия облегчает заинтересованным лица, имеющим корыстные цели задачу, поскольку конфиденциальная информация находится в открытом доступе. Именно по этой причине в России в период пандемии, а именно в декабре 2020 года была зарегистрирована утечка данных пациентов, зараженных корнавирусом COVID-19. Информация содержала данные как об отдельных лицах, так и списочные данные, затрагивающие несколько десятков или сотен лиц. В общей сложности, подвергнутыми незаконному распространению оказались персональные данные 35,5 тыс. россиян. [5]

Источником таких сведений является исследование InfoWatch, на основании которых авторы могут утверждать, что первопричиной утечки стало именно халатное отношение лиц, имеющих доступ к информационным ресурсам больниц и учреждений, которым пациенты предоставили персональные данные. Последствия такого инцидента отразились на пациентах в различных формах, например, в виде излишнего внимания со стороны представителей органов власти различных уровней или же ухудшения взаимоотношений в трудовой сфере. Так или иначе это являлось серьезным ударом для пострадавших людей.

В заключении, авторами предложены возможные решения по улучшению качества защиты персональных данных в здравоохранении. Главным и основным пунктом является снабжение медицинских учреждений системой эффективного электронного документооборота не только на федеральном, но и на районном и местном уровнях. Система автоматически должна быть оснащена средствами защиты регистрируемых данных, попадающих в оборот от взлома. Например, комплексные антивирусные программы, системы предупреждения и предотвращения вторжений и утечек данных. Активное внедрение

автоматизированных рабочих мест, в которые встроен модуль доверенной загрузки, который имеет сертификат. Его суть заключается в защите персональных компьютеров от несанкционированного доступа, а также в контроле целостности программной конфигурации устройств, на которых установлен этот модуль.

Основываясь на том, что на сегодняшний день в медицинских учреждениях используется ЕГИСЗ, мерой по повышению безопасности данных может являться внедрение единой и стандартизированной системы защиты, состоящей из определенных последовательных этапов. На сегодняшний день в современной медицине России нет такой системы. Такая платформа должны быть способна на моделирование угроз безопасности информации, определение соответствующего уровня защиты, установку и настройку средств защиты информации. Авторы считают, что при синхронизированной работе двух систем, а именно ЕГИСЗ и системы безопасности, информация, циркулирующая внутри медицинских учреждений, будет максимально защищена от хакерских атак, утечки и т.д. В свою очередь риск распространения конфиденциальных персональных данных пациентов будет сведен к минимуму.

Однако, стоит отметить, что предложенная мера не может являться гарантированным методом защиты. Авторы не исключают возникновение ошибок при практическом применении таковых систем одновременно. В первую очередь это связано с тем фактом, что управление электронным документооборотом, в том числе и в здравоохранении, осуществляет человек. Если внутри медицинской организации будут неверно определены угрозы, возникнет риск применения несоответствующего способа защиты персональных данных пациентов внутри программы. Если же специалисты расценят недостаточно высоким уровень защищенности информационной системы, и посчитают необходимым его увеличить, возникнет необходимость в применении излишних мер и установке дополнительных средств защиты. Это может привести к значительному росту стоимости внедрения и обслуживания системы.

Приведенные статистические данные и проведенное исследование позволяет сделать вывод, что сфера здравоохранения в России, поставленная в нестандартные условия, а именно в условия пандемии коронавируса COVID-19, не способна обеспечить должную защиту персональных данных граждан. В том числе и сведения о состоянии здоровья пациентов, охраняемые на законодательном уровне. [6]

В заключение можно сказать, что на сегодняшний день в сфере здравоохранения России создана и активно функционирует информационная система, однако немаловажный элемент безопасности разработан лишь на теоретическом уровне. Для осуществления защиты персональных данных нет стандартизированной формы, единой для всех медицинских

учреждений. Именно поэтому поликлиники и больницы должны самостоятельно обеспечивать защиту персональных данных своих пациентов от попадания в общий доступ, что может происходить посредством внешнего вмешательства со стороны злоумышленников или посредством внутренне халатности и безалаберности медицинских работников. Стоит отметить, что законодательно защита персональных данных строго регламентирована, однако с практической стороны это не влияет на улучшение защиты персональных данных и повышение уровня безопасности. Именно поэтому данную проблему стоит рассматривать не только с точно зрения законодательных актов, но и на практическом уровне разработать систему безопасности, используя системы защиты единые для всех медицинских учреждений.

Библиографический список

1. Программа XVIII Ассамблеи «Здоровая Москва» [сайт]. URL: https://moscowhealth.ru/ (дата обращения: 10.04.2021).

2. О персональных данных: федеральный закон №152-ФЗ от 27.07.2006 г. // КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2021. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 07.04.2021).

3. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ № 1119 от 01.11.2012 г. // КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2021. URL: http://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения 05.04.2021).

4. Об информации, информационных технологиях и о защите информации: федеральный закон №149-ФЗ от 27.07.2006 г. // КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2021. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 12.04.2021).

5. Утечки информации ограниченного доступа: отчет за 9 месяцев 2020 г.// Информационный портал INFOWATCH [сайт]. URL: https://d-russia.ru/wp-content/uploads/2020/12/infowatch_2020_9_monts_data_leak.pdf (дата обращения 12.04.2021).

6. Харлашин Р.А., Защита персональных данных в медорганизации: как обеспечить безопасность / Портал Российского врача. «Медвестник» [сайт]. [дата публ. 06.08.2020]. URL: https://medvestnik.ru/content/articles/Zashita-personalnyh-dannyh-v-medorganizacii-kak-obespechit-bezopasnost.html (дата обращения: 10.04.2021).