МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.23670/IRJ.2023.135.3

ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ОБРАБАТЫВАЕМЫЕ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Научная статья

Горбунов Н.А.[1, *], Кулешова В.[2], Коржук В.М.[3]
[1] ORCID : 0009-0004-2973-9594;
[2] ORCID : 0000-0003-1377-6003;
[3] ORCID : 0000-0002-0240-9067;
[1, 2, 3] Университет ИТМО, Санкт-Петербург, Российская Федерация

* Корреспондирующий автор (gorb-2157[at]mail.ru)

Аннотация

В статье описана систематизация подхода к формированию перечня персональных данных (ПДн), которые могут быть задействованы в обработке медицинскими информационными системами (МИС) с новыми целями и задачами при их разработке. Предложена методика формирования перечня ПДн, обрабатываемых в МИС, которые разрабатываются для выполнения нового функционала. В качестве исследовательских материалов для написания работы взяты данные из выписок моделирования угроз информационной безопасности для МИС компании «Нетрика Медицина». Описан в табличной форме полный перечень ПДн, используемых МИС. Практические результаты показывают, что во вновь разрабатываемых медицинских информационных системах состав обрабатываемых ПДн может быть сформирован по результатам анализа представленной в статье табличной форме ПДн. Теоретические результаты показывают классификационные сходства МИС. Сделан вывод, что методика формирования перечня ПДн, обрабатываемых в МИС, которые разрабатываются для выполнения новых задач, необходима к применению.

Ключевые слова: медицинские информационные системы, персональные данные.

PERSONAL DATA PROCESSED IN MEDICAL INFORMATION SYSTEMS

Research article

Gorbunov N.[1, *], Kuleshova V.[2], Korzhuk V.[3]
[1] ORCID : 0009-0004-2973-9594;
[2] ORCID : 0000-0003-1377-6003;
[3] ORCID : 0000-0002-0240-9067;
[1, 2, 3] ITMO University, Saint-Petersburg, Russian Federation

* Corresponding author (gorb-2157[at]mail.ru)

Abstract

The article describes the systematization of the approach to the formation of the list of personal data (PD) that can be involved in processing by medical information systems (MIS) with new goals and objectives in their development. The methodology of forming the list of personal data processed in MISs that are being developed to fulfil the new functionality is suggested. The research materials for writing the article are taken from the extracts of information security threat modelling for MIS of the company "Netrika Medicine". The complete list of PD used by the MIS is described in tabular form. Practical results show that in newly developed medical information systems, the composition of processed PD can be formed according to the results of analysing the tabular form of PD presented in the article. Theoretical results show the classification similarities of MIS. It is concluded that the methodology of forming a list of personal data processed in MISs that are being developed to fulfil new tasks should be applied.

Keywords: medical information systems, personal data.

Введение

Коммерческие и государственные медицинские учреждения в ежедневном режиме обрабатывают гигантские объемы конфиденциальной информации, в том числе и ПДн [1]. Обрабатываемые сведения носят высокий уровень значимости, так как в первую очередь, это сведения о состоянии самочувствия клиентов медицинских заведений, их диагнозы, способы реабилитации и методики врачевания, истории болезней и иные высоко ценимые на чёрных рынках материалы.

В ранее опубликованной статье на портале образовательного и инфо-методического проекта «Evercare.ru», посвящённого новейшим разработкам, современным мультитехнологиям и свершениям в направлениях телемедицины и ориентированного на цифру здравоохранения [2], размещен подробный рассказ о защите ПДн, с точки зрения понимания специфики информационной безопасных МИС, перечня угроз, вероятность которых высока во время хищения, видоизменения и бесконтрольных утечек в руки злоумышленников сведений, имеющих медицинский характер. Ради того, чтобы разобраться в необходимости осуществления мероприятий по исполнению технических и, безусловно важных, организационных манипуляций по обеспечению безопасности информации, требуется сгенерировать перечень ПДн, обрабатываемых МИС.

Наибольшая часть данных, обрабатываемых организациями с медицинским профилем, имеют специальную категорию ПДн [1], так как это тайны врачебной и около врачебной деятельности, находящейся в информационных системах (ИС) только с письменного разрешения пациентов или их законных представителей. Как мы знаем, согласие на обработку и дальнейшую передачу ПДн законодательством России разрешено подписывать с помощью электронно-цифровой подписи [1], соответственно в МИС также необходимо обеспечить данный момент тем более, что в продуктах компании «Нетрика Медицина» [3] этот сервис давно используется.

Целью данной статьи является разработка методики формирования перечня ПДн, обрабатываемых в МИС.

На основе методов, использовавшихся при разработке МИС, созданных и сопровождаемых компанией «Нетрика Медицина», для достижения поставленной цели была сформулирована задача по представлению перечня ПДн, обрабатываемых в МИС, которые разрабатываются для выполнения нового функционала.

При подготовке материалов для написания данной статьи использовались методы логического вывода, системного анализа, поиска и познания, а также методологического проектирования.

Новизна исследования заключается в том, что разработана новая методика для определения состава защищаемых ПДн, которые будут обрабатываться в МИС с новым функционалом. Данная методика основана на общем принципе определения перечня ПДн для ИС различного назначения, однако мы выделили определённые особенности состава ПДн, обрабатываемых в МИС.

Актуальность исследования заключается в моментах, которые мы выявили о зависимости типов и состава ПДн от типа и количественно-качественных показателей МИС, где они потенциально могут обрабатываться. Произведена работа, систематизирующая результирующие показатели в форме табличного изложения (таблица 1), которое имеет колоссальную практическую значимость при разработке перечня ПДн из состава МИС, разрабатываемых для реализации нового функционала.

Компания «Нетрика Медицина» специализируется на безопасной интеграции МИС и создании как федеральных, так и региональных сервисных функций врачебному комьюнити, обследуемым и организаторам процессов по охране и улучшению здоровья людей.

Подсистема защиты информации является встроенной в основную и разрабатывается по функциональным, целевым и задачным лекалам, предъявляемым к учреждениям с медицинской ориентированностью, и в процессе анализа материалов о методиках защищенности, моделирования угроз. После формирования технических проектов и заданий реализуемость заданных параметров информационной безопасности обеспечивают распорядительно-организационная составляющая [4], развёрнутые и функционирующие средства защиты информации (СрЗИ) и криптографические СрЗИ [5], и, несомненно, аттестация медучреждений [6] на соответствие требованиям, предъявляемым к ИС, где обрабатываются ПДн [7].

При проектировании подсистем информационной безопасности [8] медучреждений важно обеспечить защиту базы данных, порядок резервного копирования и реинкарнации как всей МИС, так и встроенных подсистем. Для автоматизированной обработки данных важна постоянная исправность программно-аппаратных составляющих работоспособности МИС, непрерывность процесса обработки информации (сохранение, передача, сбор) [9]. Наиболее значимый функционал требуется дублировать, чтобы производительность МИС не снижалась.

Важнейшим приоритетом компании «Нетрика Медицина» является содействие государству и всему врачебному сообществу в достижении долгосрочных планов в здравоохранительной сфере по средствам снабжения достоверной, полной и актуальной и информацией [10] всех участников мероприятий по предоставлению медицинской помощи.

Платформа «N3. Здравоохранение» [3] позволяет разным медорганизациям обмениваться сведениями. Главный подход заключается в том, чтобы на ведомственном уровне интеграционной платформы уже существующим медорганизациям было бы позволено интегрироваться с другими МИС и их облачными модификациями. То есть МИС будет являться рекомендованной для иных медорганизаций, использующих интеграционную шину. В рамках Федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» [11] через программный комплекс «N3. Здравоохранение» [3] происходит интеграция с ЕГИСЗ, и потенциальный формализованный обмен сведениями с государственными и региональными ИС. Также к интеграционной платформе подключаются и порталы пациентов. Данная схема (рисунок 1) уже работает в более чем двадцати региональных и федеральных МИС.

Рисунок 1 - Интеграционная платформа «N3. Здравоохранение»

DOI: https://doi.org/10.23670/IRJ.2023.135.3.1

В настоящий момент многие регионы России используют интеграционную платформу «N3. Здравоохранение» [3]. Более семидесяти пяти разработчиков МИС уже с ней интегрированы. То есть, более двадцати пяти миллионов человек обслуживаются уже подключенными медорганизациями. Изучая результаты исследования, описанные в статье, был проанализирован опыт обрабатываемых ПДн в рамках задач, осуществляемых программным комплексом «N3. Здравоохранение» [3].

Рисунок 2 - Перечень медицинских учреждений
DOI: https://doi.org/10.23670/IRJ.2023.135.3.2

Методическая ценность исследования, описанного в статье, заключается в систематизации практик разработки перечня ПДн, которые важно учесть при разработке новых МИС, как потенциальные.

Основные результаты

Принимая во внимание анализ моделей угроз информационной безопасности, разработанных в соответствии с Методикой оценки угроз безопасности информации, утвержденной ФСТЭК России 05.02.2021 года [12], для перечисленных на рисунке 2 медучреждений, особенное внимание было заострено на следующих сходствах:

1) МИС должны удовлетворять мерам защиты информации, установленным постановлением Правительства Российской Федерации № 1119 [9]. Уровень защищенности ПДн, обрабатываемых в МИС, должен быть УЗ-2;

2) МИС должны соответствовать мерам защиты информации для государственных ИС, утвержденным приказом Федеральной службы по техническому и экспортному контролю Российской Федерации № 17 [13]. Класс защищенности, установленный для МИС, должен быть К-2;

3) МИС предназначены для автоматизации [14] процессов здравоохранения.

Для практической ориентированности проведенного исследования был составлен пошаговый алгоритм формирования перечня ПДн (таблица 1).

В качестве практических рекомендаций важно отметить удобство табличной формы представления, применение которой позволяет отсекать излишние ПДн, которые не будут обрабатываться в МИС. То есть при формировании технических заданий и проектов для вновь разрабатываемых МИС рекомендуем взять за основу перечень ПДн, приведённый в таблице 1. Далее, в процессе анализа необходимости обработки различных ПДн в МИС с новым функционалом, предоставляется возможность исключить те ПДн, которые могут быть не востребованы или не являются актуальными.

Таблица 1 - Описательный набор состава ПДн

DOI: https://doi.org/10.23670/IRJ.2023.135.3.3

№	Тип	Набор ПДн	Категорирование по ПДн (ФЗ-152)
1	Личные сведения застрахованных	1) имя, отчество и фамилия; 2) половая принадлежность; 3) дата появления на свет; 4) место появления на свет; 5) подданство; 6) документ, идентифицирующий личность; 7) место проживания; 8) дата и место регистрация; 9) страховой номер индивидуального лицевого счёта (СНИЛС); 10) номер полиса обязательного медстрахования страхуемого; 11) страховая медорганизация, определенная страхуемым; 12) дата регистрации страхуемого; 13) работающий или нет статус страхуемого; 14) медорганизация для получения первичной медико-санитарной помощи	Информация, подлежащая защите (иные категории ПДн)
2	Инф-я о медпомощи	1) номер полиса обязательного медстрахования страхуемого; 2) медорганизация, оказавшая услуги; 3) виды помощи; 4) условия помощи; 5) формы помощи; 6) сроки помощи; 7) объемы помощи; 8) стоимость помощи; 9) результат оценка специалиста (диагноз); 10) профиль помощи; 11) сведения о медуслугах, оказанных застрахованному, и о назначенных лекарствах; 12) стандарты оказания медпомощи;	Информация, подлежащая защите (специальные категории ПДн [1])

		13) инф-я о медработниках, оказавших услуги; 14) результат обращения за помощью; 15) контроль условий, сроков, объемов и качества помощи	
3	Иная инф-я для оказания медуслуг и их регистрация	1) холост или нет; 2) социальный статус; 3) образование, профессия; 4) инф-я о здоровье; 5) фотопортрет; 6) идентификационный номер налогоплательщика; 7) копии документов, идентифицирующих личность (паспорт или водительское удостоверения); 8) данные, описывающие право на дополнительные льготы, гарантии и компенсации по следующим основаниям: ветеранство, инвалидность, пребывание в радиационной зоне, служба в подразделениях особого риска, семейности, беременность сотрудника, детский возраст и т.д.; 9) договор об оказании медуслуг между пациентом и медучреждением; 10) справка и акты расчетов; 11) личные обращения больных; 12) инф-я о несчастных случаях	Информация, подлежащая защите (специальные категории ПДн [1])
4	Учетные документы медицинской организации, содержащей ПДн пациентов	1) журналы ведения приёма пациентов; 2) медкарты амбулаторных больных; 3) медкарты стационарных больных; 4) результаты обследований и анализов; 5) договоры о медуслугах; 6) счета за медуслуги; 7) регистрационные журналы об обследованиях, услугах, больничных листов и д.р.; 8) заключения врачебных экспертиз	Информация, подлежащая защите (специальные категории ПДн [1])
5	Данные работников	1) имя, отчество и фамилия;	Информация, подлежащая защите

		2) должность и подразделение; 3) звание	(иные категории ПДн)
6	Инф-я о вызовах скорой и неотложной медпомощи	1) имя, отчество и фамилия; 2) паспорт, идентифицирующий личности, страховой медполис и др.; 3) возраст больного; 4) указывается работодатель при вызове; 5) серия и номер документа, идентифицирующего личность пациента (если есть); 6) детальный адрес пациента; 7) инф-я о лице, вызывающего скорую или неотложную медпомощь; 8) результат оценка специалиста (диагноз); 9) имя, отчество и фамилия специалиста, оказавшего скорую или неотложную медпомощь	Информация, подлежащая защите (специальные категории ПДн [1])
7	Данные пациентов, получивших скорую или неотложную медпомощь	1) имя, отчество и фамилия; 2) документ, идентифицирующий личности, страховой медполис и др.; 3) анамнез, объективные и субъективные данные	Информация, подлежащая защите (иные категории ПДн)

Обсуждение

При разработке МИС, создаваемых для выполнения нового ряда целей и задач, необходимо учитывать перечень обрабатываемых ПДн (в соответствии с таблицей 1), а также, что МИС являются ИС, обрабатывающими:

- ПДн специальной категории [1], описывающие самочувствие и интимные жизненные моменты пациентов;
- общедоступные ПДн [1]. Ведётся обработка ПДн пациентов, полученных из общедоступных источников ПДн;
- иные категории ПДн [1].

Конкретным примером использования разработанной методики описания перечня ПДн в базах данных МИС является формирование угроз информационной безопасности МИС компании «Нетрика Медицина». В частности, речь идёт об интеграционной платформе «N3. Здравоохранение» и её дополнительных сервисов: «Портал пациента», «Управление потоками пациентов», «Интегрированная электронная медицинская карта». В настоящий момент проведены мероприятия по составлению перечня ПДн для системы управления доступом, разработка которой будет в скором времени завершена.

На примере МИС компании «Нетрика Медицина», были выявлены результаты использования разработанной методики описания перечня ПДн в базах данных МИС, а именно определен состав чувствительных сведений, отображенный в таблице 2. В столбце «МИС» представлено наименование, а в столбцах с первого по седьмой отмечены символом «+» те ПДн из таблицы 1, состав которых актуален для конкретной исследуемой МИС.

К практическим рекомендациям использования разработанной методики описания перечня ПДн относятся работы по проектированию в защищенном исполнении МИС. То есть на этапе формирования модели угроз информационной безопасности для вышеперечисленных МИС, разработанных компанией «Нетрика Медицина», сфокусировано внимание на процедуре категорировании ПДн. Дополнительно были определены виды обрабатываемых ПДн и подчеркнута необходимость проведения дополнительных мероприятий по безопасной обработки чувствительных сведений. К таким мероприятиям были отнесены разработка эффективных организационных и технических мер по обеспечения второго уровня защищенности ПДн, обрабатываемых в МИС. При подготовке описательной модели нарушителей были определены возможные цели реализации угроз безопасности информации. В частности, было практически определено потенциальное нарушение конфиденциальности ПДн граждан, которые являются авторизированными пользователями МИС. Данный вид риска является актуальным как для внешних, так и для внутренних нарушителей, так как к ним возможно отнести различные криминальные группировки, хакеров, действующих и бывших работников.

Таблица 2 - Состав ПДн МИС компании «Нетрика Медицина»

DOI: https://doi.org/10.23670/IRJ.2023.135.3.4

МИС	1	2	3	4	5	6	7
N3. Здравоохранение	+	+	+	+	+	+	+
Портал пациента	+	+	+	-	-	+	+
Управление потоками пациентов	+	+	+	-	+	+	+
Интегрированная электронная медицинская карта	+	+	+	-	+	+	+
Система управления доступом	+	-	-	+	+	-	-

Заключение

Подводя итоги исследования, важно отметить, что подтверждены актуальность, научность, методическая и практическая ценность материалов, описывающих систематизированный подход к формированию перечня ПДн, обрабатываемых в МИС, которые разрабатываются для выполнения нового функционала. Таким образом, при разработке состава ПДн необходимо воспользоваться методикой их формирования, описанной в данной статье.

Конфликт интересов

Не указан.

Рецензия

Сообщество рецензентов Международного научно-исследовательского журнала
DOI: https://doi.org/10.23670/IRJ.2023.135.3.5

Conflict of Interest

None declared.

Review

International Research Journal Reviewers Community
DOI: https://doi.org/10.23670/IRJ.2023.135.3.5

Список литературы / References

1. Российская Федерация. Законы. О персональных данных : федеральный закон № 152-ФЗ : [принят Государственной Думой 8 июля 2006 г. : одобр. Советом Федерации 14 июля 2006 г.] // КонсультантПлюс. — URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 13.04.2023).

2. Информационная безопасность в здравоохранении: основные аспекты // EverCare. — 2022. — URL: https://evercare.ru/news/informacionnaya-bezopasnost-v-zdravookhranenii-osnovnye-aspekty?fbclid=IwAR04mAgphtQy1feml0MHjTUn_5mBbASoO-0vxmC63H-1EkGoh6A9rhuHybM (дата обращения: 13.06.2023).

3. Программные продукты компании «Нетрика Медицина» // Нетрика.Медицина. — 2023. — URL: https://n3med.ru/ (дата обращения: 13.06.2023)

4. ГОСТ Р 7.0.97-2016. Организационно-распорядительная документация. Требования к оформлению документов. — Введ. 2016-12-08. — М.: Стандартинформ, 2018. — 15 с.

5. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. — Введ. 2006-12-27. — Москва: Стандартинформ, 2008. — 12 с.

6. Российская Федерация. Об утверждении порядка аттестации объектов информатизации и особенностях его реализации : Информационное сообщение Федеральной службы по техническому и экспортному контролю от 29 апреля 2021 г. № 240/24/2087 // Электронный фонд правовых и нормативно-технических документов. — URL: https://docs.cntd.ru/document/607749878 (дата обращения: 13.04.2023).

7. Российская Федерация. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : Постановление Правительства РФ от 1 ноября 2012 г. № 1119 // Правительство России. — URL: http://government.ru/docs/all/84743/ (дата обращения: 13.04.2023).

8. ГОСТ Р ИСО/МЭК 21827-2010. Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса. — Введ. 2010-10-30. — Москва: Стандартинформ, 2015. — 124 с.

9. ГОСТ 20886-85. Организация данных в системах обработки данных. — Введ. 1986-07-01. — Москва: Стандартинформ, 2005. — 8 с.

10. Российская Федерация. О внесении изменений в государственную программу Российской Федерации «Развитие здравоохранения» и признании утратившим силу постановления Правительства Российской Федерации от 28 сентября 2020 г. № 1549 : Постановление Правительства Российской Федерации от 23 декабря 2020 г. № 2225 // Правительство России. — URL: http://government.ru/docs/all/131726/ (дата обращения: 13.04.2023).

11. Федеральный проект «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» // Министерство здравоохранения Российской Федерации. — 2019. — URL: https://minzdrav.gov.ru/poleznye-resursy/natsproektzdravoohranenie/tsifra (дата обращения: 13.04.2023).

12. Методический документ. Методика оценки угроз безопасности информации. — Утвержден ФСТЭК России 05 февраля 2021 г. // ФСТЭК России. — URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 13.04.2023).

13. Российская Федерация. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ ФСТЭК России от 11 февраля 2013 г. № 17 // ФСТЭК России. — URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 13.04.2023).

14. ГОСТ 27878-88. Системы и комплексы медицинские автоматизированные. — Введ. 1989-07-01. — Москва: Государственный комитет СССР по стандартам, 1989. — 15 с.

Список литературы на английском языке / References in English

1. Rossijskaja Federacija. Zakony. O personal'nyh dannyh [Russian Federation. Laws. On Personal Data] : federal Law № 152-FZ : [accepted by State Duma on July 8, 2006 : approved by Federation Council on July 14, 2006] // Consultant. — URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (accessed: 13.04.2023). [in Russian]

2. Informatsionnaja bezopasnost' v zdravoohranenii: osnovnye aspekty [Information Security in Healthcare: Main Aspects] // EverCare. — 2022. — URL: https://evercare.ru/news/informacionnaya-bezopasnost-v-zdravookhranenii-osnovnye-aspekty?fbclid=IwAR04mAgphtQy1feml0MHjTUn_5mBbASoO-0vxmC63H-1EkGoh6A9rhuHybM (accessed: 13.06.2023). [in Russian]

3. Programmnye produkty kompanii «Netrika Medicina» [Software products of the company «Netrika Medicine»] // Netrika.Medicine. — 2023. — URL: https://n3med.ru/ (accessed: 13.06.2023) [in Russian]

4. GOST R 7.0.97-2016. Organizacionno-rasporjaditel'naja dokumentacija. Trebovanija k oformleniju dokumentov [Organizational and administrative documentation. Requirements for document preparation]. — Introduced 2016-12-08. — M.: Standartinform, 2018. — 15 p. [in Russian]

5. GOST R 50922-2006. Zaschita informatsii. Osnovnye terminy i opredelenija [Data Protection. Basic Terms and Definitions]. — Introduced 2006-12-27. — Moscow: Standartinform, 2008. — 12 p. [in Russian]

6. Rossijskaja Federacija. Ob utverzhdenii poryadka attestacii ob"ektov informatizacii i osobennostyah ego realizacii [Russian Federation. On the approval of the procedure for attestation of informatization objects and the features of its implementation] : Information message of the Federal Service for Technical and Export Control dated April 29, 2021 № 240/24/2087 // Electronic fund of legal, regulatory and technical documents. — URL: https://docs.cntd.ru/document/607749878 (accessed: 13.04.2023). [in Russian]

7. Rossijskaja Federacija. Ob utverzhdenii trebovanij k zashchite personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh [Russian Federation. On Approval of the Requirements for the Protection of Personal Data during Their Processing in Personal Data Information Systems] : Decree of the Government of the Russian Federation dated Nivember 1, 2012 № 1119 // Government of Russia. — URL: http://government.ru/docs/all/84743/ (accessed: 13.04.2023). [in Russian]

8. GOST R ISO/MEK 21827-2010. Informatsionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Proektirovanie sistem bezopasnosti. Model' zrelosti protsessa [GOST R ISO/IEC 21827-2010. Information Technology. Methods and Means of Ensuring Security. Design of Security Systems. Process Maturity Model]. — Introduced 2010-10-30. — Moscow: Standartinform, 2015. — 124 p. [in Russian]

9. GOST 20886-85. Organizatsija dannyh v sistemah obrabotki dannyh [GOST 20886-85. Organization of Data in Data Processing Systems]. — Introduced 1986-07-01. — Moscow: Standartinform, 2005. — 8 p. [in Russian]

10. Rossijskaja Federacija. O vnesenii izmenenij v gosudarstvennuyu programmu Rossijskoj Federacii «Razvitie zdravoohraneniya» i priznanii utrativshim silu postanovleniya Pravitel'stva Rossijskoj Federacii ot 28 sentyabrya 2020 g. [Russian Federation. On Amending the State Program of the Russian Federation "Health Development" and Recognizing Decree of the Government of the Russian Federation of September 28, 2020 № 1549 as invalid] : Decree of the Government of the Russian Federation dated December 23, 2020 № 2225 // Gevernment of Russia. — URL: http://government.ru/docs/all/131726/ (accessed: 13.04.2023). [in Russian]

11. Federal'nyj proekt «Sozdanie edinogo cifrovogo kontura v zdravoohranenii na osnove edinoj gosudarstvennoj informacionnoj sistemy v sfere zdravoohraneniya (EGISZ)» [Federal project "Creation of a Unified Digital Contour in Healthcare Based on a Unified State Information System in the Field of Healthcare"] // Ministry of Health of the Russian Federation. — 2019. — URL: https://minzdrav.gov.ru/poleznye-resursy/natsproektzdravoohranenie/tsifra (accessed: 13.04.2023). [in Russian]

12. Metodicheskij dokument. Metodika ocenki ugroz bezopasnosti informacii [Methodical document. Methodology for assessing threats to information security]. — Approved by the Federal Service for Technical and Export Control of Russia on February 5, 2021 // FSTEC of Russia. — URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (accessed: 13.04.2023). [in Russian]

13. Rossijskaja Federacija. Ob utverzhdenii Trebovanij o zashchite informacii, ne sostavlyayushchej gosudarstvennuyu tajnu, soderzhashchejsya v gosudarstvennyh informacionnyh sistemah [Russian Federation. On Approval of the Requirements for the Protection of Information That Is Not a State Secret Contained in State Information Systems] : Order of the Federal Service for Technical and Export Control of Russia dated February 11, 2013 №17] // FSTEC of Russia. — URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (accessed: 13.04.2023). [in Russian]

14. GOST 27878-88. Sistemy i kompleksy meditsinskie avtomatizirovannye [GOST 27878-88. Medical Automated Systems and Complexes]. — Introduced 1989-07-01. — Moscow: USSR State Committee for Standards, 1989. — 15 p. [in Russian]