

СТОЛБОВ А.П.,

д.т.н., профессор, ФГАОУ ВО «Первый московский государственный медицинский университет им. И.М. Сеченова» Минздрава России (Сеченовский университет), г. Москва, Россия,
e-mail: ap100Lbov@mail.ru

К ВОПРОСУ ОБ ОРГАНИЗАЦИИ ОБЕЗЛИЧИВАНИЯ И ИСПОЛЬЗОВАНИЯ ДАННЫХ РЕАЛЬНОЙ КЛИНИЧЕСКОЙ ПРАКТИКИ

DOI: 10.25881/18110193_2025_2_32

Аннотация. Рассмотрены требования к обезличенным данным реальной клинической практики (ДРКП), основные методы обезличивания и синтетизации ДРКП, позволяющие сохранить их клиническую информативность. Приведено описание процедуры сбора, обезличивания и использования ДРКП, которая обеспечивает высокую стойкость обезличенных данных относительно угроз нарушения конфиденциальности сведений, составляющих врачебную тайну.

Ключевые слова: данные реальной клинической практики, защита персональных данных, обезличивание персональных данных, информационные технологии.

Для цитирования: Столбов А.П. К вопросу об организации обезличивания и использования данных реальной клинической практики. Врач и информационные технологии. 2025; 2: 32-53. DOI: 10.25881/18110193_2025_2_32.

STOLBOV A.P.,

DSc, professor, The First Sechenov Moscow State Medical University,
Moscow, Russia, e-mail: ap100Lbov@mail.ru

ON THE ISSUE OF DEPERSONALIZATION AND USE OF REAL-WORLD DATA

DOI: 10.25881/18110193_2025_2_32

Abstract. *The requirements to anonymized real-world data (RWD), basic methods of anonymization and synthetization of RWD that allow to preserve their clinical informativeness are considered. The description of the procedure of collection, anonymization and use of RWD is given, which provides high stability of anonymized data in relation to threats of breach of confidentiality of information constituting medical confidentiality.*

Keywords: *real-world data, personal data protection, depersonalization of personal data, information technology.*

For citation: *Stolbov A.P. On the issue of depersonalization and use of real-world data. Medical doctor and information technology. 2025; 2: 32-53. DOI: 10.25881/18110193_2025_2_32.*

Одной из актуальных задач цифровой трансформации здравоохранения [1] является формирование экосистемы сбора, обработки и использования данных реальной клинической практики (ДРКП) (real-world data, RWD), в том числе для получения на их основе доказательств эффективности и безопасности медицинских технологий (real-world evidence, RWE), выполнения научных исследований, разработки систем поддержки принятия врачебных (клинических) и управленческих решений.

Специфика работы с ДРКП, полученными из электронных медицинских карт (ЭМК), реестров и регистров пациентов основана на потенциальной возможности разглашения сведений, составляющих врачебную тайну, и их использования для причинения вреда субъектам персональных данных — пациентам (здесь и далее под пациентом будем понимать физическое лицо, о котором осуществляется сбор сведений о состоянии его здоровья и оказанной ему медицинской помощи). Поэтому особое внимание при работе с такими данными должно уделяться обеспечению их конфиденциальности — защищенности от несанкционированного доступа. Одним из способов выполнения этого требования является обезличивание данных, под которым понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить их принадлежность конкретному субъекту персональных данных (ст. 3 Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных», далее — закон № 152-ФЗ). В октябре 2024 г. Советом Евразийской экономической комиссии были приняты рекомендации по развитию регулирования обращения лекарственных средств в части сбора, анализа и использования ДРКП [2], в которых одним из ключевых требований является обезличивание таких данных. При этом государствам-участникам предложено разработать единые принципы доверенного обезличивания и повторного использования первичных медицинских данных из систем ведения ЭМК, систем удаленного мониторинга пациентов, программных средств для автоматизации назначения лекарственной терапии и других информационных систем для целей формирования наборов ДРКП, а также рекомендовано на законодательном уровне разрешить контролируемый

оборот обезличенных медицинских данных для целей проведения исследований реальной клинической практики.

Следует заметить, что в соответствии с частью 2.1 статьи 10 закона № 152-ФЗ обработка персональных данных, касающихся состояния здоровья, полученных в результате обезличивания, без согласия пациента или его законного представителя допускается только в целях повышения эффективности государственного или муниципального управления, в том числе государственного контроля качества и безопасности медицинской деятельности, фармаконадзора, а также в иных целях, предусмотренных экспериментальными правовыми режимами [3, 4]. При этом во всех случаях должна быть обеспечена защита обезличенных данных от несанкционированного доступа, изменения и удаления.

Летом 2024 г. в закон № 152-ФЗ были внесены изменения [5] (вступают в силу с 01.09.2025 г.) — добавлена статья 13.1 «Особенности обработки персональных данных, полученных в результате обезличивания персональных данных, при формировании составов персональных данных и предоставлении доступа к ним», в которой описана централизованная модель сбора и обработки наборов (составов) обезличенных данных, в том числе о состоянии здоровья, с использованием для этого единой государственной информационной системы (ГИС), оператором которой является Минцифры России.

Как показал наш анализ требований к организации обработки и использования обезличенных данных, перечисленных в ст. 13.1, а также изложенных в постановлениях Правительства РФ [6–9], указанная выше ГИС не может быть использована для сбора и работы с ДРКП, поскольку, как сказано в ст. 13.1, обработка обезличенных составов данных пользователями может выполняться только в этой ГИС. Запись, извлечение, передача, распространение составов данных из указанной ГИС запрещены. Система ориентирована прежде всего на решение задач государственного управления, и в ней, скорее всего, не будут реализованы такие специфические для ДРКП функции и сервисы, как обработка медицинских изображений, записей биосигналов (ЭКГ, ЭЭГ), формирование и разметка датасетов клинических данных, используемых при

разработке и валидации систем поддержки принятия врачебных решений, оценке медицинских технологий и т. п. Заметим, что сейчас в ГИС предусмотрено формирование составов обезличенных данных, полученных только от операторов мобильной связи, записи которых содержат: обезличенный идентификатор абонента, его год рождения (с возможностью выбора определенного временного интервала), пол, гражданство, местоположение, включая информацию об изменении местоположения абонента с определенной периодичностью, а также возможностью определения страны абонента, находящегося на территории РФ в международном роуминге [10].

Целью настоящей работы является анализ и обсуждение требований к организации сбора, обезличивания и использования ДРКП.

Необходимо определить требования к обезличенным данным, принципы организации их сбора, обработки и использования, выбрать методы обезличивания сведений, содержащихся в электронных медицинских документах (картах), регистрах и реестрах — источниках ДРКП. В данной работе мы не будем рассматривать вопросы качества ДРКП (достоверности, точности и полноты), это отдельная тема [11–13].

Как показали исследования [14–18], основными требованиями к процедурам сбора, обезличивания, накопления и использования ДРКП являются:

1) возможность сбора, интеграции и дополнения новыми сведениями (обогащения) обезличенных данных, относящихся к одному и тому же пациенту, полученных из разных источников и(или) в разное время на протяжении продолжительного периода (без выполнения процедуры деобезличивания), в условиях возможных изменений его идентификационных данных: перемены Ф.И.О., замены документов, удостоверяющих личность, а также изменения даты рождения, например, в целях обеспечения тайны усыновления (не более чем на три месяца) относительно фактической даты рождения, что предусмотрено ст. 135 Семейного кодекса РФ; заметим также, что с 24.07.2023 г. в РФ введен запрет на смену пола, что было разрешено и осуществлялось ранее (ст. 45.1 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» № 323-ФЗ от

21.11.2011 г.; далее — закон № 323-ФЗ); при этом первичными источниками данных для обезличивания являются ЭМК пациентов;

- 2) идентифицируемость данных, означающая возможность установления принадлежности данных конкретному пациенту (персоне) при их получении из разных источников и(или) в разное время, в том числе при использовании разных идентификаторов пациента;
- 3) обеспечение уникальности данных о пациенте в условиях множественности источников их получения и возможного при этом дублирования информации. Это предполагает применение специальных процедур для выявления повторов и несогласованности полученной информации, которая при этом может быть представлена в разных форматах, с разными гранулярностью и уровнем формализации: в виде неструктурированного и структурированного текста, в кодированном виде [19], в виде наборов данных с записью биосигналов (ЭКГ, ЭЭГ), диагностических изображений (рентгеновские, КТ-, МРТ- и УЗИ-снимки), фото, видео- и аудиозаписей (далее — файлы инструментальных исследований, ФИИ);
- 4) сохранение при обезличивании исходной информативности темпоральных клинических данных, привязанных к календарным датам и, возможно, ко времени суток (здесь и далее под информативностью данных будем понимать возможность извлечения из данных информации, необходимой для решения определенных задач);
- 5) обеспечение возможности санкционированной обратной персонификации (деобезличивания, реидентификации) — предоставление авторизованным пользователям идентификационных (персональных) данных о пациентах в строго определенных случаях.

Как показано в ГОСТ Р 55036 [20], выполнение первого, второго и пятого требований возможно только при использовании для сокрытия информации о пациенте и обозначения (маркировки) относящейся к нему обезличенной информации единого уникального идентификатора — псевдонима пациента, который присваивается ему централизованно и остается неизменным в течение всего периода сбора информации о нём. При этом очевидно, что

необходимо отслеживать и учитывать возможные изменения персональных данных пациента в течение этого периода: перемены Ф.И.О., замены документов, удостоверяющих личность и т. д. (необходимость ведения истории изменений).

Кроме того, должны быть обеспечены высокая стойкость обезличенных данных относительно угроз несанкционированной реидентификации, а также защищенность данных от несанкционированного доступа, искажения и удаления на всех этапах сбора, обработки и использования, в соответствии с актуальными угрозами и требованиями к информационной безопасности, установленными нормативными документами.

Требования, касающиеся возможности получения разнородной клинической и административной информации из множества разных источников в течение продолжительного времени, в свою очередь, предполагают максимальную технологическую нейтральность форматов представления и обмена данными, обусловленную необходимостью взаимодействия с информационными системами, реализованными на разных программно-аппаратных платформах, а также их возможную замену в течение жизненного цикла обезличенных данных.

Далее будем рассматривать процессы обезличивания только структурированных данных — записей и документов, и будем полагать, что состав и виды атрибутов в записях соответствуют второму (section-level templates) или третьему (entry-level templates) уровню формализации по ГОСТ Р ИСО/HL7 27932 [19] (здесь и далее под атрибутом будем понимать элемент структуры данных, соответствующий определенной семантической единице информации). При этом будем рассматривать три категории атрибутов:

- идентифицирующие пациента (Personally Identifiable Information, PII) [21]: Ф.И.О., дата и место рождения, адреса регистрации и места жительства, реквизиты паспорта (свидетельства о рождении), иные прямые идентификаторы пациента (СНИЛС, номер полиса ОМС, ИНН), номер медицинской карты и т. п.;
- административные данные (атрибуты), содержащие сведения о медицинской организации, о медицинских работниках, о месте (адресе) оказания медицинской помощи,

реквизиты (номера, даты, названия) отдельных медицинских документов;

- клинические данные — атрибуты, описывающие состояние здоровья пациента: анамнез(ы), результаты (протоколы) осмотра, лабораторных и инструментальных исследований (включая ссылки на ФИИ), медицинские вмешательства и иные клинические события и факты, в том числе о неблагоприятных реакциях и побочных действиях при применении лекарственных препаратов, донорской крови, биомедицинских клеточных продуктов и медицинских изделий; клинические данные имеют темпоральный характер; к этой же категории относятся и медико-административные данные (атрибуты) о пациенте: о постановке (снятии) на динамическое наблюдение и(или) диспансерный учет; о включении в нозологические и социальные («льготы») регистры и т. п.

ФИИ также будем относить к клиническим данным. При этом заметим, что сегодня могут использоваться сразу несколько разных форматов данных для представления одного и того же вида исследований, например, ЭКГ [22].

МАТЕРИАЛЫ И МЕТОДЫ

В настоящее время разработаны и используются разные методы обезличивания [15, 23–25] (см. также стандарт ISO/IEC 20889 [26]). В стандарте ГОСТ Р 55036 определено понятие «псевдонимизация» медицинских данных (соответствует термину «обезличивание» в законе № 152-ФЗ) и описаны основные модели организации псевдонимизации, а также рассмотрены угрозы (риски) несанкционированной реперсонификации таких данных. В 2013 г. приказом Роскомнадзора № 966 [27] были утверждены требования по обезличиванию персональных данных в государственных и муниципальных органах, и изданы методические рекомендации по его применению [28] (в марте 2025 г. Роскомнадзором был опубликован проект нового приказа, взамен приказа № 996 [29]). В июне 2018 г. приказом Минздрава России № 341н [30] был утвержден порядок обезличивания сведений, обрабатываемых в подсистеме «Федеральная интегрированная электронная медицинская карта» (ФИЭМК) Единой государственной информационной системе в сфере здравоохранения (ЕГИСЗ) [31], а в марте 2025 г.

взамен него был подписан новый приказ № 139н [32] (вступает в силу 01.09.2025), в которых описаны правила (алгоритмы) формирования идентификатора (псевдонима) пациента, сведений о дате и месте его рождения, месте жительства и месте регистрации при обезличивании (одинаковы в обоих приказах).

Обычно при обезличивании медицинских данных используются сразу несколько методов сокрытия информации об объектах идентификации — пациентах, медицинских работниках, медицинских организациях, адресах и т. д. (см. таблицу 1), что позволяет снизить риски несанкционированной реидентификации.

Таблица 1 — Методы обезличивания медицинских данных

Метод \ Описание метода	Применение при обезличивании
1	2
1. Введение идентификаторов	
Замена (замещение) части сведений (атрибутов) об объекте идентификатором с созданием «секретной» таблицы соответствия (справочника) идентификаторов объекта. Справочник хранится отдельно от обезличенных данных	Метод применяется для сокрытия информации о пациенте, для чего ему присваивается псевдоидентификатор (псевдоним), который используется для маркировки относящейся к пациенту информации в обезличенном наборе данных. Метод может применяться также для сокрытия информации о медицинских организациях, медицинских работниках и иных объектах идентификации, например, об адресах, населенных пунктах и т.п.
2. Изменение состава и(или) семантики атрибутов	
Удаление, искажение (смещение, замена значений) или изменение (округление, осреднение значений) части атрибутов	Обычно применяется для представления адресов, дат и других показателей (атрибутов). Не применяется для атрибутов, используемых для представления результатов физикального осмотра, лабораторных и инструментальных исследований, параметров медицинского вмешательства (доза, количество, продолжительность и т.п.), результатов (исходов) лечения и иных клинических событий и фактов
3. Преобразование	
Обобщение значений атрибутов (при этом изменяется семантика атрибута)	Может применяться для «загрубления» значений атрибута, например: указание вместо кода диагноза только класса заболеваний; вместо полного адреса — только названия населенного пункта; вместо возраста — возрастной группы (при этом количество групп может быть разным)
4. Декомпозиция (разделение)	
Разделение множества атрибутов на несколько подмножеств с созданием таблиц связей между подмножествами, с последующим раздельным хранением записей, соответствующих подмножествам	При решении задач, связанных с аналитической обработкой обезличенных данных, требуется предварительная сборка атрибутов из нескольких подмножеств с помощью таблицы связей. Может применяться для повышения защищенности конфиденциальной информации при хранении в базах данных, в том числе в сочетании с шифрованием данных
5. Перемешивание	
Перестановка отдельных значений или групп значений атрибутов данных по определенному алгоритму	Возможно три вида перемешивания атрибутов: а) горизонтальное — перестановка значений атрибутов, относящихся к одному объекту идентификации; б) вертикальное — перестановка значений атрибутов, относящихся к разным объектам; в) смешанное — сочетание а) и б). При решении задач, связанных с аналитической обработкой обезличенных данных, требуется предварительное восстановление «привязки» значений атрибутов к объектам идентификации. При обезличивании медицинских данных практически не используется

Как видим, при применении метода изменения состава или семантики атрибутов и метода преобразования в ряде случаев возможно снижение информативности обезличенного набора данных по сравнению с исходным необезличенным.

Как показано в работах [23, 33, 34], эффективным способом защиты от несанкционированной реперсонификации является модификация значений атрибутов, используемых в составе квазидентификаторов — комбинации (набору) атрибутов в записи, позволяющей выделить пациента в массиве данных (например: дата рождения + пол + место жительства — см. ISO/IEC 20889 [26]), которая может осуществляться путем: а) обобщения (например, указание вместо полного адреса только названия населенного пункта); и(или) б) смещения на "секретную" величину, не известную нарушителю — лицу, осуществляющему попытку несанкционированной реперсонификации обезличенных данных.

При выборе методов обезличивания медицинских данных следует исходить из того, что состав и информативность атрибутов в обезличенных наборах данных определяют возможный перечень решаемых с их использованием научных, управленческих и иных задач, а также методы их решения. Кроме того, применимость тех или иных методов обезличивания зависит также от вида атрибутов и уровня формализации информации: неструктурированный или структурированный по определенным разделам (полям) текст, коды, даты, числа, массивы измерительной информации, изображения, видео, аудио и т.д.

РЕЗУЛЬТАТЫ

Исходя из перечисленных выше требований, обращение обезличенных ДРКП предлагается организовать на основе:

- централизованной модели сбора, обезличивания (псевдонимизации), накопления, хранения и предоставления доступа авторизованным пользователям к обезличенным наборам (составам) данных; создания и использования для этого единой государственной централизованной платформы (ЕП) как подсистемы в составе ЕГИСЗ (например, как развитие ФИЭМК); при этом сбор и обезличивание медицинских данных осуществляется

только об идентифицированных пациентах, имеющих российское гражданство; информация о пациентах, которым медицинская помощь была оказана анонимно, а также о неидентифицированных пациентах не собирается;

- ведения единой сводной (интегральной) базы псевдонимизированных медицинских данных (СБД), полученных от медицинских организаций; внесение (загрузка) информации в СБД осуществляется в аддитивном, инкрементном режиме — путем последовательного добавления информации о новых пациентах либо новой, дополнительной информации о пациенте, данные о котором были загружены в базу ранее (обогащение данных);
- минимизации состава сведений, хранимых в СБД — не хранить в ней данные, которые можно получить (восстановить) из официальных публичных источников, регистров и реестров (например, из федерального реестра медицинских и фармацевтических организаций (ФРМО));
- разделения функций и полномочий доступа субъектов, в том числе пользователей, к персональным и клиническим данным пациентов, а также к сведениям о медицинских организациях;
- применения всеми субъектами программных средств, выполняющих обезличивание по единым правилам (требованиям к обезличиванию) и прошедших процедуру оценки соответствия (сертификации) требованиям к средствам защиты информации (статья 19 закона № 152-ФЗ).

Субъектами, участвующими в формировании обезличенных наборов ДРКП, являются (рисунок 1):

- поставщики первичных ДРКП — медицинские организации, которые имеют доступ к персональным и клиническим данным своих пациентов, но доступа к псевдонимам пациентов и псевдонимизированным данным не имеют;
- оператор псевдонимизации (ОП), который выполняет три функции: 1) присваивает пациенту, сведения о котором содержатся в наборах ДРКП, уникальный идентификатор — псевдоним; 2) ведет «секретный» справочник псевдонимов пациентов (СПП) (см. далее);

3) в необходимых, строго определенных случаях предоставляет авторизованным пользователям идентификационные персональные данные пациента. ОП имеет доступ к персональным данным пациентов и их псевдонимам; доступа к исходным клиническим данным пациентов (к сведениям, составляющим врачебную тайну), а также к псевдонимизированным наборам данных не имеет;

- оператор ЕП, осуществляющий в процессе обезличивания прием и обработку информации от медицинских организаций и ОП, формирование сводного набора обезличенных ДРКП (СБД), формирование на основе СБД наборов (составов) данных (СДн) и предоставление к ним доступа авторизованным пользователям; оператор ЕП не имеет доступа к персональным данным пациентов.

Пользователями обезличенных наборов ДРКП являются:

- органы исполнительной власти в сфере здравоохранения, в том числе осуществляющие государственный контроль (надзор) за безопасностью медицинской деятельности, фармаконадзор, мониторинг безопасности донорской крови и ее компонентов, биомедицинских клеточных продуктов и медицинских

изделий, государственные внебюджетные фонды, а также и уполномоченные ими организации (далее – органы управления, ОУ);

- организации, осуществляющие научные исследования, разработку новых медицинских технологий, фармацевтической продукции, медицинских изделий, а также программного обеспечения (далее – организации-разработчики, ОР).

Формирование наборов ДРКП медицинскими организациями осуществляется по заданиям (запросам) ОУ. Запрос на обезличивание может содержать:

- временной период оказания медицинской помощи (наблюдения пациента);
- половозрастные и(или) иные категории пациентов (в том числе «все»);
- медицинские критерии для отбора случаев оказания медицинской помощи (нозологические единицы, виды медицинских вмешательств, применяемые лекарственные препараты, медицинские изделия, биомедицинские клеточные продукты и т.д.).

Кроме того, в запросе может быть указан состав сведений, включаемых в обезличенный набор данных (состав данных). При этом очевидно, что перечень управленческих, научных и иных

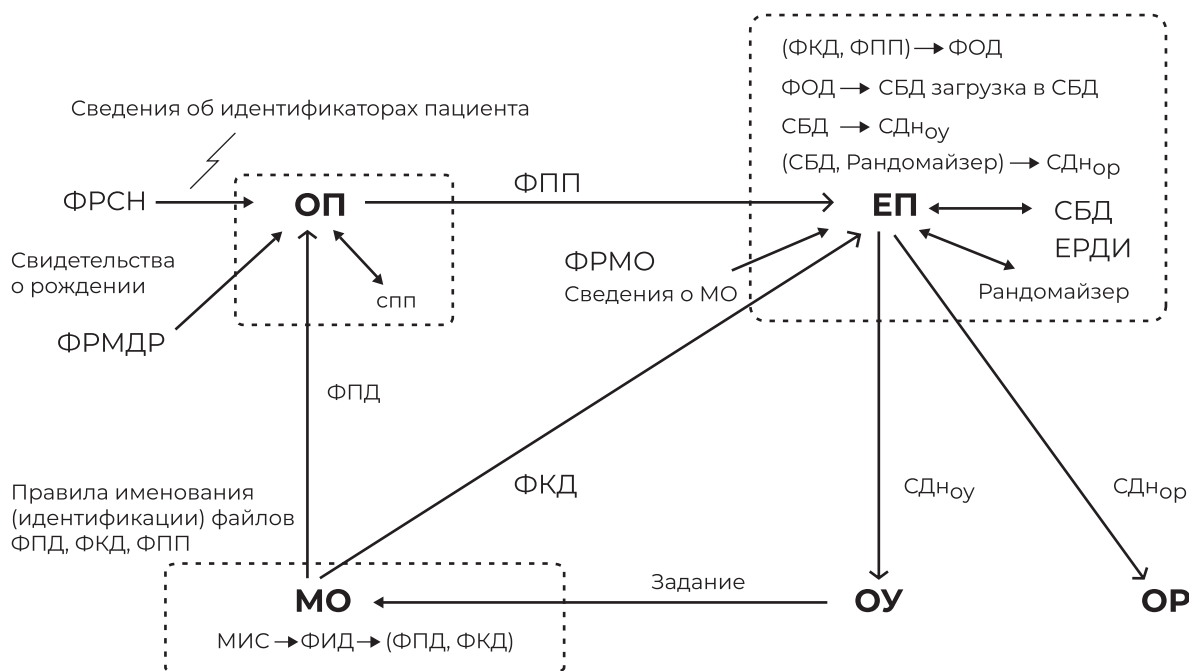


Рисунок 1 — Схема взаимодействия субъектов при сборе и обезличивании ДРКП.

задач, решаемых с использованием обезличенных данных («аналитический потенциал» набора), определяется: составом атрибутов, уровнем их формализации, а также полнотой охвата случаев оказания медицинской помощи, сведения о которых представлены в обезличенном наборе данных (репрезентативностью выборки). Перечень случаев, когда осуществляется сбор и обезличивание ДРКП, а также составы обезличенных данных, должны быть определены Правительством РФ (это отдельная тема, мы не будем её касаться). Некоторые сценарии использования псевдонимизированных ДРКП, в том числе при анализе информации о побочных действиях лекарственных препаратов, приведены в ГОСТ Р 55036 [20].

ПРОЦЕДУРА СБОРА И ОБЕЗЛИЧИВАНИЯ ДРКП

Процесс цикла обезличивания и загрузки данных в СБД состоит из нескольких технологических этапов, на каждом из которых формируются временные (технологические) файлы (пакет файлов), с помощью которых осуществляется взаимодействие между субъектами (рисунок 1). На заключительном этапе цикла обезличивания выполняется загрузка очередной порции (набора) обезличенных данных в СБД. Процесс обезличивания, включая присвоение псевдонимов пациентам и загрузку (внесение) сведений в СБД, осуществляется в автоматическом режиме.

Каждый из файлов пакета представляется в виде реестра, структурно-логической единицей которого является запись о пациенте — совокупность атрибутов, относящихся к одному, определенному пациенту (считается, что файл содержит только одну запись о пациенте). Указанные атрибуты сгруппированы и расположены в записи в хронологическом порядке в соответствии с едиными стандартами представления информации, унифицированными с форматами структурированных электронных медицинских документов (СЭМД) (см. таблицу 2, в которой приведены обозначения и семантика атрибутов, а также перечислены атрибуты в записях соответствующего файла; знак «плюс» в графе означает обязательное наличие атрибута в записи файла, буква «у» — при необходимости). Все файлы имеют одинаковое количество записей — по количеству пациентов, сведения о

которых содержатся в файлах. Каждой записи в файле присваивается уникальный идентификатор (номер) — случайное число либо порядковый номер записи в последовательном файле. Во всех файлах запись о конкретном пациенте имеет один и тот же номер. Каждому файлу присваивается уникальный составной идентификатор (имя файла), включающий: ОГРН медицинской организации, дату и порядковый номер сформированного в этот день пакета файлов. Имя файла используется для координации и синхронизации потоков файлов между субъектами в процессе (цикле) сбора, обезличивания и загрузки в СБД.

Обезличивание осуществляется путем удаления, изменения и замены сведений об объектах идентификации — пациентах, медицинских работниках и медицинских организациях посредством применения метода введения идентификаторов и метода изменения состава и семантики данных.

При обезличивании из записей исходного набора данных удаляются все атрибуты, позволяющие идентифицировать пациента и медицинского работника, в том числе реквизиты медицинских документов, сведения о его законных представителях и т. д. Пациенту присваивается уникальный идентификатор-псевдоним, который формируется централизованно ОП. Псевдоним вычисляется путем выполнения следующих действий:

- 1) формируется символьная строка, являющаяся конкатенацией атрибутов: вид документа (код) удостоверения личности + его серия и(или) номер;
- 2) к этой символьной строке справа добавляется уникальное 10-значное случайное число, генерируемое для каждого пациента;
- 3) для полученной таким образом символьной строки вычисляется хеш (например, хеш, вычисляемый по алгоритму, описанному в ГОСТ Р 34.11-2012 [35]), значение которого и используется в качестве псевдонима пациента (подобный алгоритм формирования псевдонима описан в приказах Минздрава России № 341н и № 139н).

При вычислении псевдонима для новорожденного ребенка, не зарегистрированного в органах ЗАГС, используются реквизиты его медицинского свидетельства о рождении.

Таблица 2 — Атрибуты в записях файлов (наборов, базы данных)

№	Название (семантика) атрибута \ группы атрибутов	ФИД	ФКД	ФПД	ФПП	ФОД	СПП
1	2	3	4	5	6	7	8
Атрибуты в исходных данных							
1. Формируются медицинской организацией							
1.1	персональные данные пациента: Ф. И. О., реквизиты документа, удостоверяющего его личность, СНИЛС, номер полиса ОМС и др.	+		+			+
1.2	пол пациента	+		+	+	+	+
1.3	фактическая дата рождения пациента	+		+			+
1.4	фактическая дата смерти пациента	у		у			у
1.5	адреса места регистрации и места жительства пациента	+					
1.6	ОГРН медицинской организации	+	+	+			
1.7	наименование медицинской организации	+					
1.8	адрес подразделения медицинской организации, где была оказана медицинская помощь	+					
1.9	атрибуты для описания клинических событий (фактов) (привязаны к датам и, возможно, ко времени суток)	+	+			+	
1.10	фактические даты клинических событий (фактов)	+	+				
1.11	Ф.И.О. медицинского работника(ов)	+					
1.12	название должности медицинского работника(ов)	+					
1.13	номера медицинских документов \ записей в регистрах	+					
1.14	ссылки на ФИИ (с персональными данными пациента)	у					
1.15	сведения о матери ребенка: Ф.И.О., дата рождения, реквизиты паспорта, СНИЛС, номер полиса ОМС	у					у
Атрибуты, формируемые при обезличивании							
2. Формируются медицинской организацией							
2.1	номер записи о пациенте в файлах ФКД, ФПД, ФПП		+	+	+		
2.2	названия (коды) населённых пунктов регистрации \ проживания пациента		+			+	
2.3	название (код) населенного пункта оказания медпомощи		+			+	
2.4	код должности медицинского работника(ов)		+			+	
2.5	ссылки на обезличенные ФИИ		у			у	
3. Формируются оператором псевдонимизации ОП							
3.1	псевдоним пациента				+	+	+
3.2	константа смещения дат (целое число со знаком)				+		+
3.3	смещенные даты рождения \ смерти пациента				+	+	+
3.4	номер записи о пациенте в ФРСН						у
3.5	история изменений персональных данных пациента						у
4. Формируются оператором единой платформы ЕП							
4.1	смещенные даты клинических событий (фактов)					+	
4.2	ссылки на обезличенные ФИИ в ЕРДИ					у	
4.3	даты начала и конца периода, за который в СБД имеются сведения о пациенте (с учетом смещения дат)					в СБД	

Применение случайного числа обеспечивает уникальность псевдонима, а также невозможность его компрометации путем вычисления (подбора) на основе известных реквизитов документа удостоверения личности пациента. Заметим, что уникальный псевдоним пациента

может быть сформирован и другим способом [15]. К изменяемым (заменяемым) атрибутам относятся (см. таблицу 2):

- адреса места регистрации и места жительства пациента и места оказания медицинской помощи (подразделения медицинской

организации) — вместо них указываются только названия населенных пунктов, либо их коды по государственному адресному реестру (атрибуты 2.2 и 2.3);

- все даты: дата рождения, дата смерти пациента, даты событий, связанных с оказанием медицинской помощи (даты госпитализации, выписки, перевода, осмотра, выполнения инструментальных и лабораторных исследований, процедур, манипуляций, операций и т.п.) — указываются со смещением на «константу смещения дат» (целое число со знаком), которая вычисляется для каждого пациента при присвоении ему псевдонима. Константа вычисляется по следующему алгоритму: если остаток от деления по «модулю три» случайного числа, сгенерированного при вычислении псевдонима пациента, равен нулю, то константа равна «минус один день»; если остаток равен одному, то константа равна «плюс один день»; если остаток равен двум, то константа равна «плюс два дня». Рассчитанная таким образом константа сохраняется в справочнике псевдонимов пациентов СПП (см. далее).

Вычисление смещенной даты при обезличивании выполняется по правилам «арифметики календарных дат»: если константа смещения дат равна «минус один день», то фактическая дата уменьшается на один день; если равна «плюс один день», то к дате добавляется один день; если константа равна «плюс два дня» — к дате добавляется два дня. При смещении даты могут измениться также календарный месяц и год. При обезличивании изменяются все даты, относящиеся к пациенту, включая даты его рождения и смерти (далее этот метод будем называть методом рандомного смещения дат).

К неизменяемым при обезличивании сведениям относятся атрибуты, используемые для представления пола пациента, а также клинических данных о пациенте: диагнозы, результаты физикального осмотра, инструментальных и лабораторных исследований, применяемые лекарственные препараты, иные виды медицинских вмешательств, параметры медицинского вмешательства (доза, количество, продолжительность и т. п.), а также атрибуты, используемые для указания времени суток в темпоральных клинических данных (в таблице 2 не показаны).

Процедура (цикл) обезличивания состоит из нескольких этапов (рисунок 1, таблица 2):

1. Медицинская организация при получении задания:

- а) на основе информации в МИС (в ЭМК, в полицевых регистрах) в соответствии с критериями, указанными в задании, формирует исходный персонифицированный набор данных — файл исходных данных (ФИД);
- б) затем на основе ФИД формируется файл клинических данных (ФКД); при этом выполняется первичное обезличивание: в ФКД не включаются атрибуты, идентифицирующие пациента, в качестве идентификатора используется номер записи о нем (атрибут 2.1 в таблице 2); вместо сведений о медработнике указывается только код его должности (атрибут 2.4); вместо сведений о медицинской организации указывается только её ОГРН (атрибут 1.6); вместо адресов места регистрации и места жительства пациента, и адреса медицинской организации указываются только названия (коды по ГРН) населённых пунктов (атрибуты 2.2 и 2.3); указываются фактические даты (атрибуты 1.10), связанные с оказанием медицинской помощи пациенту;
- в) формирует файл персональных данных (ФПД), содержащий записи о пациентах, сведения о которых включены в ФИД; записи файла содержат атрибуты, необходимые для присвоения псевдонима пациенту, а также для идентификации пациента при возможных изменениях его Ф.И.О., даты рождения и реквизитов документа, удостоверяющего личность;
- г) передает файл ФПД ОП, а файл ФКД — оператору ЕП.

2. ОП при получении от медицинской организации файла ФПД:

- а) для каждого пациента, сведения о котором включены в ФПД, проверяет наличие записи о нем в справочнике псевдонимов пациентов СПП (проверка на уникальность пациента); при отсутствии записи о пациенте в СПП формирует для него псевдоним (атрибут 3.1), константу смещения дат (атрибут 3.2), вычисляет смещенные даты рождения и смерти (при необходимости) (атрибуты 3.3), и вносит сведения о новом пациенте в справочник;
- б) формирует файл псевдонимов пациентов (ФПП), записи которого содержат атрибуты из

СПП, необходимые для дальнейшего обезличивания, и передает ФПП оператору ЕП.

Записи СПП содержат: псевдоним пациента; Ф.И.О.; пол; дату рождения; дату смерти; вид и реквизиты документа, удостоверяющего личность; номер полиса ОМС и СНИЛС (при наличии); константу смещения дат; номер записи о пациенте в федеральном регистре сведений о населении (ФРСН); историю изменений персональных данных пациента (получение свидетельства о рождении в органах ЗАГС; получение, замена паспорта; изменение Ф.И.О.). Кроме этого, записи СПП содержат также служебные атрибуты: ОГРН медицинской организации, на основе данных от которой был сформирован псевдоним пациента и дату его присвоения.

Доступ к справочнику СПП имеют только специально уполномоченные сотрудники ОП. Доступ иных лиц к информации в справочниках и её передача кому-либо категорически запрещены за исключением случаев, предусмотренных законодательством Российской Федерации, в том числе при необходимости предоставления сведений об объектах идентификации авторизованным пользователям в строго определенных случаях, перечень которых должен быть определен Правительством РФ.

3. Оператор ЕП при получении ФКД и ФПП от медицинской организации и ОП:

- а) на основе ФПП и ФКД формирует файл обезличенных данных (ФОД), выполняя при этом «дообезличивание» данных: сдвигает все даты клинических фактов, указанные в записях ФКД, на константу смещения дат (атрибут 3.2), указанную в записи ФПП с тем же номером (атрибут 2.1), — вычисляет атрибуты смещенных дат (п. 4.1); номер записи о пациенте заменяет его псевдонимом (атрибут 3.1); вносит в запись о пациенте атрибут пола (атрибут 1.2) и смещенные даты рождения и смерти пациента (атрибуты 3.3);
- б) загружает файл ФОД в СБД, при этом: выполняет проверку записей на наличие повторов («дублей»), в том числе по датам и источникам сведений (медицинским организациям); и при отсутствии коллизий дополняет записи пациентов в СБД новыми сведениями о состоянии его здоровья и полученной

медицинской помощи, содержащимися в ФОД, либо вносит сведения о новом пациенте в СБД; в записи о каждом пациенте в СБД содержатся смещенные даты начала и конца периода, за который в ней имеются сведения о пациенте (атрибуты 4.3). Заметим, что клинические данные и иные сведения о пациенте могут поступать и загружаться в СБД не обязательно строго в хронологическом порядке;

- в) по завершении загрузки в СБД (включая проверку связности данных), актуализирует метаданные об информации, хранящейся в СБД.

По завершении цикла обработки временные ФИД, ФПД, ФКД, ФПП и ФОД удаляются всеми операторами.

ИСПОЛЬЗОВАНИЕ ОБЕЗЛИЧЕННЫХ ДАННЫХ

Предоставление доступа к информации, содержащейся в СБД, осуществляется оператором ЕП по запросам авторизованных пользователей путем выгрузки и формирования СДн. Запрос на формирование и предоставление СДн в общем случае может содержать те же параметры, что и в заданиях на обезличивание.

СДн для государственных органов, внебюджетных фондов и уполномоченных ими ОУ по составу атрибутов в записях могут быть полностью идентичны записям в СБД; при этом записи маркируются единым псевдонимом пациента, содержат ОГРН медицинских организаций, а также названия (коды) населенных пунктов, где была оказана медицинская помощь и проживают пациенты. При необходимости, требуемые сведения о медицинской организации могут быть получены пользователями ОУ из ФРМО по её ОГРН.

При формировании обезличенных составов данных для ОР должна быть предусмотрена возможность сокрытия информации о медицинских организациях и названиях населенных пунктов, а также полная анонимизация сведений о пациентах, исключающая возможность соотнесения записей в этих составах данных с записями в СБД и в наборах данных для государственных органов и учреждений, а также с записями в файлах, формируемых и передаваемых медицинскими организациями оператору ЕП. Выполнение этого требования осуществляется путем

необратимой анонимизации и синтетизации атрибутов в записях при формировании обезличенного набора (состава) данных на основе выборки из СБД:

- замены атрибутов: а) псевдоним пациента, б) ОГРН медицинской организации, в) название (код по государственному адресному реестру) населенного пункта — на сгенерированный рандомайзером уникальный условный номер; при этом для каждого состава (набора) данных формируются свои уникальные в пределах этого набора номера пациентов, медицинских организаций и населенных пунктов — одному и тому же населенному пункту во всех записях набора соответствует один и тот же уникальный номер (аналогично и для номеров медицинских организаций);
- дополнительного случайного сдвига всех смещенных дат, относящихся к пациенту, новые значения которых вычисляются по следующему алгоритму: для каждого пациента генерируется случайное число, затем вычисляется остаток от его деления по модулю три и все даты сдвигаются относительно ранее смещенных дат: на «на минус три дня», если остаток равен нулю; на «плюс три дня», если остаток равен единице; на «плюс два дня», если остаток равен двум.

При необходимости, при формировании СДн в него могут быть включены также данные о категории (номенклатуре, уровне) медицинской организации (на основе сведений из ФРМО), например, в виде специального атрибута, содержащего соответствующий классификационный код медицинской организации.

Поскольку при формировании таких наборов изменение и замена атрибутов осуществляется случайным образом и необратимо, то вероятность реперсонификации наборов (составов) данных, предоставляемых разработчикам, снижается практически до нуля. Это возможно только при наличии доступа к персональным данным пациентов в результате их утечки в процессе обезличивания. По сути такой набор данных можно считать синтетическим, поскольку все даты в его записях получены путем двойного случайного сдвига, и любое совпадение с данными о реальных пациентах является исключительно случайным.

В составе ЕП могут быть предусмотрены специальные сервисы (функции) для пользователей наборов (составов) обезличенных данных, в том числе, например, для подготовки запросов на формирование СДн, аналитической обработки и визуализации данных, содержащихся в СДн, а также функции, предусмотренные для реализации в подсистеме ФИЭМК (формирование и разметка датасетов и др.).

ОБСУЖДЕНИЕ

Рассмотрим некоторые аспекты, связанные с используемыми методами обезличивания, а также с реализацией описанной выше централизованной модели контролируемого обращения обезличенных ДРКП.

Информативность темпоральных клинических данных. Указание в обезличенных данных фактических дат (даты рождения, дат клинических событий и фактов), а также сведений о конкретных медицинских организациях и медицинских работниках в общем случае повышает риск несанкционированной реидентификации. В тоже время, при «загрублении» даты клинически значимого события (факта), например, при указании только года, как это предусмотрено приказом Минздрава России № 139н при обезличивании данных в ФИЭМК, или только года и месяца существенно снижается информативность обезличенных темпоральных клинических данных, что делает практически невозможным их использование при решении задач, связанных с анализом динамики состояния пациента, течения и лечения болезни, в том числе, например, в целях фармаконадзора.

Применение случайного смещения всех фактических дат, включая дату рождения пациента, в сочетании с другими методами обезличивания, во-первых, обеспечивает высокую стойкость обезличенных данных относительно угроз реперсонификации сведений, составляющих врачебную тайну, и, во-вторых, позволяет полностью сохранить исходную информативность темпоральных клинических данных (атрибутов), какой она была до обезличивания.

Ведение справочника псевдонимов пациентов. Как уже было отмечено выше, в случае продолжительного периода сбора ДРКП, Ф.И.О. и реквизиты документа, удостоверяющего личность пациента, используемые для

идентификации пациента и указанные в учетных медицинских документах, могут изменяться. В связи с этим, при ведении справочника псевдонимов СПП ОП регулярно получает информацию (см. схему):

- о получении (замене) документа удостоверения личности пациента, получении СНИЛС, перемене Ф.И.О., изменении даты рождения, а также о смерти пациента — от оператора ФРСН [36], коим является ФНС России (сведения предоставляются в режиме рассылки [37]). Заметим, что в ФРСН нет сведений о медицинском свидетельстве о рождении, на основе которого органами ЗАГС было оформлено свидетельство о рождении;
- о регистрации ребенка в едином государственном реестре ЗАГС из федерального реестра медицинских документов о рождении [38, 39]: дата регистрации; Ф.И.О. и пол ребенка; реквизиты свидетельства о рождении; реквизиты медицинского свидетельства о рождении (дата, номер, кем выдано), на основании которого проведена регистрация.

При получении информации об изменении даты рождения в целях сохранения тайны усыновления, изменение дат, в том числе даты рождения, в наборах данных не производится, поскольку это не влияет на достоверность и аналитическую информативность атрибутов, используемых для представления темпоральной клинической информации о пациенте. Следует отметить, что номер полиса ОМС и СНИЛС остаются неизменными в течение всей жизни гражданина — они могут изменяться только при смене пола или даты рождения. При этом СНИЛС присваивается Социальным фондом России всем российским гражданам в беззаявительном порядке, сразу после регистрации рождения ребенка в едином государственном реестре ЗАГС (информации об этом поступает в Социальный фонд России в автоматическом режиме).

Функции ОП мог бы выполнять Федеральный фонд ОМС, который в режиме рассылки получает от оператора ФРСН сведения о всех изменениях в идентификации пациентов (по постановлению Правительства РФ от 09.10.2021 № 1723).

Использование информации из медицинских регистров и от фондов ОМС. Помимо медицинских организаций поставлять данные для обезличивания и загрузки в СБД могут также

операторы нозологических и иных медицинских регистров [40–42], а также фонды ОМС. Например, информацию о результатах экспертизы качества медицинской помощи, а также данные об оплате медицинской помощи, с указанием соответствующих клинко-статистических групп или видов высокотехнологичной медицинской помощи. Кроме того, источником данных для обезличивания и загрузки в СБД мог бы быть и цифровой медицинский профиль пациента, создание которого предусмотрено федеральным проектом «Национальная цифровая платформа «Здоровье»» [43].

Обезличивание текстовой информации. Основным источником ДРКП являются ЭМК пациентов. При этом в условиях рутинной практики клинические факты не регистрируются в ЭМК с тем же уровнем детализации, как это принято при проведении клинических исследований и испытаний, содержат большой объем неструктурированной информации, пропуски и ошибки в данных [12, 13]. Автоматическое извлечение и кодирование информации из текстовых записей в ЭМК сегодня пока ещё связано с определенными трудностями [44]. Поскольку в неструктурированных текстовых записях могут встречаться персональные данные пациентов при обезличивании информации, извлекаемой из ЭМК, эти сведения необходимо удалить из текстов, причем без снижения клинической информативности текстов для дальнейшего анализа [45]. При этом следует учитывать необходимость выделения и смещения (изменения) дат, например, в тексте анамнеза или эпикриза, для чего необходим специальный сервис или приложение (модуль).

Обезличивание и использование данных инструментальных исследований. При необходимости вместе с обезличенными протоколами инструментальных исследований в составе ФКД оператору ЕП могут быть направлены также соответствующие обезличенные ФИИ (на схеме это не показано). В составе СБД должно быть предусмотрено специальное хранилище обезличенных ФИИ — единый репозиторий обезличенных данных инструментальных исследований (ЕРДИ). Записи ФКД должны содержать ссылки на эти обезличенные ФИИ. При обезличивании идентификатор исходного ФИИ, указанный в записи ФИД, заменяется на уникальный

идентификатор (имя) соответствующего обезличенного ФИИ. Правила формирования таких имен должны обеспечивать невозможность их сопоставления с идентификаторами исходных ФИИ.

ФИИ хорошо структурированы — в них явно выделены атрибуты, содержащие идентификационные данные пациентов. Однако такие файлы могут содержать также атрибуты с дополнительной клинической информацией в виде текста [46, 47]. Как правило, эта информация, а также сведения о дате исследования и иные административные данные, содержится также в протоколе исследования, поэтому при обезличивании ФИИ эти атрибуты могут быть удалены — в заголовке обезличенного ФИИ достаточно оставить только уникальный номер этого файла, ссылка на который указана в обезличенном протоколе исследования. Полагаем, что удаление из заголовка ФИИ указанных атрибутов обеспечивает практическую невозможность обратной персонификации файла на основе его контента — диаграммы (ЭКГ, ЭЭГ), изображения, видеозаписи эндоскопического исследования и т. д. Общие требования и некоторые рекомендации о процедурах обезличивания файлов приведены в ГОСТ Р ИСО/МЭК 27038 [48], а также в ГОСТ Р 71674 [49] для файлов в формате DICOM.

Предоставление доступа пользователей, относящихся к категории ОР, к обезличенным ФИИ осуществляется вместе с соответствующими анонимизированными протоколами исследований с рандомными условными номерами пациентов и медицинских организаций, а также с рандомно смещенными датами рождения пациента, выполнения исследования и т. д. (см. выше). При этом названия (идентификаторы) обезличенных ФИИ и ссылки на них в протоколах также должны необратимо изменяться с использованием рандомизатора (случайного числа), что сделает невозможным их сопоставление с обезличенными ФИИ из ЕРДИ.

Для выполнения перечисленных выше требований должны быть унифицированы, стандартизованы и опубликованы: форматы исходных (электронных медицинских документов, реестров и регистров) и обезличенных наборов данных, в том числе форматы контейнеров (файлов), используемых для обмена данными; правила кодирования информации, а также

правила (алгоритмы) обезличивания. Кроме того, необходимо разработать стандарты метаданных, описывающих обезличенные наборы ДРКП, в том числе единые правила идентификации (именования) таких наборов данных и контейнеров.

Обработку и апробацию технологий сбора, обезличивания и использования ДРКП целесообразно осуществлять в рамках пилотного проекта на ограниченном составе участников с привлечением частных компаний, имеющих соответствующие ресурсы и опыт, и введением специального экспериментального правового режима.

ЗАКЛЮЧЕНИЕ

1. Разделение функций и полномочий доступа субъектов к персональным идентификационным и медицинским данным при сборе, обезличивании, накоплении и использовании ДРКП на основе централизованной модели и единой цифровой платформы, а также перечисленные выше способы сокрытия информации при обезличивании, по нашему мнению, позволят:
 - обеспечить высокую стойкость обезличенных данных относительно угроз нарушения конфиденциальности сведений, составляющих врачебную тайну;
 - снизить совокупные затраты субъектов на ИТ-обеспечение и защиту информации в процессе сбора и обращения обезличенных ДРКП.
2. Применение при обезличивании метода рандомного смещения дат:
 - обеспечивает сохранение исходной информативности темпоральных клинических данных, что позволяет использовать обезличенные данные для решения задач, связанных с анализом динамики состояния пациента, течения и лечения болезни, в том числе в целях фармаконадзора;
 - является одним из эффективных способов защиты от реперсонификации, при сборе и дальнейшем использовании обезличенных ДРКП.
3. Синтетизация наборов обезличенных ДРКП путем двойного рандомного смещения дат и замены псевдонимов пациентов, ОГРН

медицинских организаций и названий населенных пунктов на их условные «случайные» номера позволяет:

- полностью сохранить информативность:
 - а) данных, необходимых для анализа и исследования потоков и маршрутизации различных категорий пациентов при тех или иных состояниях и заболеваниях, в том числе с учетом вида (номенклатуры, уровня, классификации) медицинских организаций; б) темпоральных клинических данных, необходимых для исследования динамики состояния пациента, течения и лечения болезни, в том числе с учетом этапности и преемственности оказания медицинской помощи в разных медицинских организациях;
- исключить какую-либо возможность соотнесения записей в наборе с данными о реальных пациентах.

Описанные выше процедура и методы обезличивания и синтетизации обеспечивают полную анонимность и сохранение исходной информативности собранных ДРКП, применение которых, по нашему мнению, позволит

построить единую, гибкую и удобную систему контролируемого оборота обезличенных ДРКП, в том числе с целью их исследования и получения доказательств эффективности и безопасности медицинских технологий, а также разработки и верификации программного обеспечения, предназначенного для интерпретации данных и принятия решений, в том числе с использованием технологий искусственного интеллекта.

Выше были описаны только самые общие принципы и методы обезличивания ДРКП. Не рассмотрены многие важные вопросы, в частности, связанные с построением модели угроз их информационной безопасности (подходы к построению такой модели описаны в ГОСТ Р 55036 [20]), количественной оценкой рисков восстановления персональной принадлежности обезличенных данных [33, 34, 50] и другие.

Автор будет признателен всем, кто пришлет свои замечания и предложения по рассмотренным вопросам по электронной почте на адрес ap100Lbov@mail.ru.

Конфликт интересов. Автор декларирует отсутствие конфликта интересов. Работа не имела спонсорской поддержки.

ЛИТЕРАТУРА/REFERENCES

1. Распоряжение Правительства Российской Федерации от 17.04.2024 №959-р «Об утверждении стратегического направления в области цифровой трансформации здравоохранения на 2024–2030 годы». [Rasporyazhenie Pravitel'stva Rossijskoj Federacii ot 17.04.2024 №959-r «Ob utverzhdenii strategicheskogo napravleniya v oblasti tsifrovoy transformatsii zdavookhraneniya na 2024–2030 gody». (In Russ.)]
2. Рекомендации Совета Евразийской экономической комиссии от 18.10.2024 №1 «Об общих подходах к развитию регулирования обращения лекарственных средств в рамках Евразийского экономического союза в части сбора, анализа и использования данных реальной клинической практики». [Rekomendacii Soveta Evrazijskoj ehkonomicheskoy komissii ot 18.10.2024 №1 «Ob obshchikh podkhodakh k razvitiyu regulirovaniya obrashcheniya lekarstvennykh sredstv v ramkakh Evrazijskogo ehkonomicheskogo soyuza v chasti sбора, analiza i ispol'zovaniya dannykh real'noj klinicheskoy praktiki». (In Russ.)]
3. Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» №123-ФЗ от 24.04.2020. [Federal'nyj zakon «O provedenii ehksperimenta po ustanovleniyu special'nogo regulirovaniya v celyakh sozdaniya neobkhodimykh uslovij dlya razrabotki i vnedreniya tekhnologij iskusstvennogo intellekta v sub'ekte Rossijskoj Federacii - gorode federal'nogo znacheniya Moskve i vnesenii izmenenij v stat'i 6 i 10 Federal'nogo zakona «O personal'nykh dannykh» №123-FZ ot 24.04.2020. (In Russ.)]
4. Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» №258-ФЗ от 31.07.2020. [[Federal'nyj zakon «Ob ehksperimental'nykh pravovykh rezhimakh v sfere cifrovyykh innovacij v Rossijskoj Federacii» №258-FZ ot 31.07.2020. (In Russ.)]

5. Федеральный закон «О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» от 08.08.2024 №233-ФЗ. [Federal'nyj zakon «O vnesenii izmenenij v Federal'nyj zakon «O personal'nykh dannyxh» i Federal'nyj zakon «O provedenii ehksperimenta po ustanovleniyu special'nogo regulirovaniya v celyakh sozdaniya neobkhodimyykh uslovij dlya razrabotki i vnedreniya tekhnologij iskusstvennogo intellekta v sub'ekte Rossijskoj Federacii - gorode federal'nogo znacheniya Moskve i vnesenii izmenenij v stat'i 6 i 10 Federal'nogo zakona «O personal'nykh dannyxh» ot 08.08.2024 №233-FZ. (In Russ.)]
6. Проект Постановления Правительства Российской Федерации «О государственной информационной системе, предназначенной для обработки персональных данных, полученных в результате обезличивания персональных данных, и внесении изменений в постановление Правительства Российской Федерации от 14 мая 2021 № 33» (ID проекта 01/01/02-25/00154662 от 14.02.2025). [Proekt Postanovleniya Pravitel'stva Rossijskoj Federacii «O gosudarstvennoj informacionnoj sisteme, prednaznachennoj dlya obrabotki personal'nykh dannyxh, poluchennykh v rezul'tate obezlichivaniya personal'nykh dannyxh, i vnesenii izmenenij v postanovlenie Pravitel'stva Rossijskoj Federacii ot 14 maya 2021 №733» (ID proekta 01/01/02-25/00154662 ot 14.02.2025) (In Russ.)]
7. Проект Постановления Правительства Российской Федерации «Об утверждении правил проверки соответствия пользователей государственной информационной системы, определенной в соответствии с частью 2 статьи 13.1 Федерального закона «О персональных данных», требованиям, указанным в части 7 статьи 13.1 Федерального закона «О персональных данных», и о внесении изменений в некоторые акты Правительства Российской Федерации (ID проекта 01/01/02-25/00154667 от 14.02.2025 г.). [Proekt Postanovleniya Pravitel'stva Rossijskoj Federacii «Ob utverzhdenii pravil proverki sootvetstviya pol'zovatelej gosudarstvennoj informacionnoj sistemy, opredelennoj v sootvetstvii s chast'yu 2 stat'i 13.1 Federal'nogo zakona «O personal'nykh dannyxh», trebovaniyam, ukazannym v chasti 7 stat'i 13.1 Federal'nogo zakona «O personal'nykh dannyxh», i o vnesenii izmenenij v nekotorye akty Pravitel'stva Rossijskoj Federacii (ID proekta 01/01/02-25/00154667 ot 14.02.2025 g.) (In Russ.)]
8. Проект Постановления Правительства Российской Федерации «Об установлении Правил взаимодействия федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, с операторами, обрабатывающими персональные данные, в целях формирования составов персональных данных, полученных в результате обезличивания персональных данных, сгруппированных по определенному признаку, при условии, что последующая обработка таких данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных» (ID проекта 01/01/02-25/00154910 от 21.02.2025). [Proekt Postanovleniya Pravitel'stva Rossijskoj Federacii «Ob ustanovlenii Pravil vzaimodejstviya federal'nogo organa ispolnitel'noj vlasti, osushchestvlyayushchego funkcii po vyrabotke i realizacii gosudarstvennoj politiki i normativno-pravovomu regulirovaniyu v sfere informacionnykh tekhnologij, s operatorami, obrabatyvayushchimi personal'nye dannye, v celyakh formirovaniya sostavov personal'nykh dannyxh, poluchennykh v rezul'tate obezlichivaniya personal'nykh dannyxh, sgruppirovannykh po opredelennomu priznaku, pri uslovii, chto posleduyushchaya obrabotka takikh dannyxh ne pozvolit opredelit' prinadlezhnost' takikh dannyxh konkretnomu sub'ektu personal'nykh dannyxh» (ID proekta 01/01/02-25/00154910 ot 21.02.2025) (In Russ.)]
9. Проект Постановления Правительства Российской Федерации «Об установлении требований к обезличиванию персональных данных, методов и правил обезличивания персональных данных» (ID проекта 02/07/04-25/00156232 от 13.04.2025). [Proekt Postanovleniya Pravitel'stva Rossijskoj Federacii «Ob ustanovlenii trebovanij k obezlichivaniyu personal'nykh dannyxh, metodov

- i pravil obezlichivaniya personal'nykh dannykh» (ID proekta 02/07/04-25/00156232 ot 13.04.2025). (In Russ.)]
10. Постановление Правительства Российской Федерации от 24.04.2025 №538 «Об утверждении перечня случаев формирования составов персональных данных, полученных в результате обезличивания персональных данных, сгруппированных по определенному признаку, при условии, что последующая обработка таких данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных». [Postanovlenie Pravitel'stva Rossijskoj Federacii ot 24.04.2025 №538 «Ob utverzhdenii perechnya sluchaev formirovaniya sostavov personal'nykh dannykh, poluchennykh v rezul'tate obezlichivaniya personal'nykh dannykh, sgruppirovannykh po opredelennomu priznaku, pri uslovii, chto posleduyushchaya obrabotka takikh dannykh ne pozvolit opredelit' prinadlezhnost' takikh dannykh konkretnomu sub'ektu personal'nykh dannykh». (In Russ.)]
 11. Гусев А.В., Зингерман Б.В., Тюфилин Д.С., Зинченко В.В. Электронные медицинские карты как источник данных реальной клинической практики // Реальная клиническая практика: данные и доказательства. — 2022. — №2(2). — С.8-20. [Gusev AV, Zingerman BV, Tyufilin DS, Zinchenko VV. Electronic medical records as a source of real-world clinical data. Real-World Data & Evidence. 2022; 2(2): 8-20. (In Russ.)] doi: 10.37489/2782-3784-myrwd-13.
 12. Ермакова Н.А., Гусев А.В., Реброва О.Ю. Ошибки в данных реальной клинической практики: обзор литературы // Врач и информационные технологии. — 2024. — №1. — С.28-43. [Ermakova NA, Gusev AV, Rebrova OYu. Errors in real-world data: a review. Medical doctor and information technology. 2024; 1: 28-43. (In Russ.)] doi: 10.25881/18110193_2024_1_28.
 13. Андрейченко А.Е., Кафтанов А.Н., Гусев А.В. Методика оценки качества данных электронных медицинских карт // Врач и информационные технологии. — 2024. — №4. — С.48-59. [Andreychenko AE, Kaftanov AN, Gusev AV. Methodology for assessing the quality of electronic medical records data. Medical doctor and information technology. 2024; 4: 48-59. (In Russ.)] doi: 10.25881/18110193_2024_4_48.
 14. Столбов А.П., Кузнецов П.П. Современные модели организации использования персональных данных о состоянии здоровья // Проблемы стандартизации в здравоохранении. — 2010. — №1-2. — С.19-24. [Stolbov AP, Kuznetsov PP. Modern models of the organization of the use of personal health data. Health care Standardization Problems. 2010; 1-2: 19-24. (In Russ.)]
 15. Столбов А.П. Обезличивание персональных данных в здравоохранении // Врач и информационные технологии. — 2017. — №3. — С.76-91. [Stolbov AP. De-identification of Personal data in Health care. Medical doctor and information technology. 2017; 3: 76-91 (In Russ.)]
 16. Гольдина Т. А., Суворов Н. И. Исследования рутинной клинической практики: от получения данных к оценке медицинских технологий и принятию решений в здравоохранении // Медицинские технологии. Оценка и выбор. — 2018. — №1(31). — С.21-29. [Goldina TA, Suvorov NI. Real-World Data Studies: from Data to Health Technology Assessment and Decision-Making in Healthcare. Medical Technologies. Assessment and Choice. 2018; 1(31): 21-29. (In Russ.)] doi: 10.17116/medtech20234501150.
 17. Мотринчук А.Ш., Касимова А.Р., Новодережкина Е.А. Руководство NICE по работе с данными из реальной клинической практики // Реальная клиническая практика: данные и доказательства. — 2022. — №2(4). — С.34-44. [Motrinchuk AS, Kasimova AR, Novoderezhkina EA. NICE guidance to working with real-world data. Real-World Data & Evidence. 2022; 2(4): 34-44. (In Russ.)] doi: 10.37489/2782-3784-myrwd-25.
 18. Радаева К.С., Пчелинцев М.В. Анализ подходов FDA по использованию данных электронных медицинских карт и данных о медицинских претензиях для поддержки принятия регуляторных решений // Реальная клиническая практика: данные и доказательства. — 2023. — №3(3). — С.28-35. [Radaeva KS, Pchelintsev MV. Analyzing FDA's approaches to using electronic health record and medical claims data to support regulatory decision making. Real-World Data & Evidence. 2023; 3(3): 28-35. (In Russ.)] doi: 10.37489/2782-3784-myrwd-39.
 19. ГОСТ Р ИСО/HL7 27932-2015. Информатизация здоровья. Архитектура клинических документов HL7. Выпуск 2. Доступно по: <https://docs.cntd.ru/document/1200135009>. Ссылка действительна

- на 10.05.2025. [GOST R ISO/HL7. Data Exchange Standards . HL7 Clinical Document Architecture, Release 2. // Available at: <https://docs.cntd.ru/document/1200135009>. Accessed 10.05.2025. (In Russ.)]
20. ГОСТ Р 55036-2012 (ISO/TS 25237:2008). Информатизация здоровья. Псевдонимизация. Доступно по: <https://docs.cntd.ru/document/1200100339>. Ссылка действительна на 10.05.2025. [GOST R 55036-2012 (ISO/TS 25237:2008). Health informatics. Pseudonymization. Available at: <https://docs.cntd.ru/document/1200100339>. Accessed 10.05.2025. (In Russ.)]
 21. ГОСТ ISO / IEC 29100-2021. Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных. Доступно по: <https://docs.cntd.ru/document/1200180230>. Ссылка действительна на 10.05.2025. [GOST ISO / IEC 29100-2021. Information technology. Security techniques. Privacy protection fundamentals. Available at: <https://docs.cntd.ru/document/1200180230>. Accessed 10.05.2025. (In Russ.)]
 22. Шутов Д.В., Попов А.А., Шулькин И.М., Ахметов Р.Н., Дроздов Д.В., Морозов С.П. Обеспечение идентичности среды регистрации и описания ЭКГ при использовании оборудования разных производителей // Врач и информационные технологии. — 2022. — №1. — С.50-61. [Shutov DV, Popov AA, Shulkin IM, Akhmetov RN, Drozdov DV, Morozov SP. Technical tests of the hardware and software complex for electrocardiogram recording and processing. Medical doctor and information technology. 2022; 1: 50-61. (In Russ.)]
 23. Саксонов Е. А., Шередин Р. В. Процедура обезличивания персональных данных // Машиностроение и компьютерные технологии. –2011. — №3. [Saksonov EA, Sheredin RV. The procedure of depersonalization of personal data. Mechanical engineering and computer technologies. 2011; 3. (In Russ.)]
 24. Столбов А.П. О стандартизации методов псевдонимизации персональных данных в здравоохранении // Проблемы стандартизации в здравоохранении. — 2017. — №9-10. — С.19-24. [Stolbov AP. On standardization of methods of pseudonymization of personal data in Health care. Standartization problems. 2017; 9-10: 19-24 (In Russ.)] doi: 10.26347/1607-2502201709-10025-036.
 25. Бабак Н.Г., Белорыбкин Л.Ю., Оцоков Ш.А., Теренин А.А., Шаброва А.И. Автоматическое обезличивание конфиденциальной информации // Russian Technological Journal. — 2023. — №11(5). — С.7-18. [Babak NG, Belorybkin LYu, Otsokov ShA, Terenin AA, Shabrova AI. Automatic depersonalization of confidential information. Russ. Technol. J. 2023; 11(5): 7-18. (In Russ.)] doi: 10.32362/2500-316X-2023-11-5-7-18.
 26. ISO/IEC 20889:2018. Privacy enhancing data de-identification terminology and classification of techniques. Доступно по: <https://www.iso.org/standard/69373>. Ссылка действительна на 10.05.2025. [ISO/IEC 20889:2018. Privacy enhancing data de-identification terminology and classification of techniques. Available at: <https://www.iso.org/standard/69373>. Accessed 10.05.2025.]
 27. Приказ Роскомнадзора от 05.09.2013 №996 «Об утверждении требований и методов по обезличиванию персональных данных». [Prikaz Roskomnadzora ot 05.09.2013 №996 «Ob utverzhdenii trebovanij i metodov po obezlichivaniyu personal'nykh dannykh». (In Russ.)]
 28. Методические рекомендации по применению приказа Роскомнадзора №996 от 05.09.2013. Утверждены 13.12.2013. [Metodicheskie rekomendacii po primeneniyu prikaza Roskomnadzora №996 ot 05.09.2013. Utverzhdeny 13.12.2013. (In Russ.)]
 29. Проект приказа Роскомнадзора «Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных» (ID проекта 02/08/03-25/00155867 от 27.03.2025) [Proekt prikaza Roskomnadzora «Ob utverzhdenii trebovanij k obezlichivaniyu personal'nykh dannykh i metodov obezlichivaniya personal'nykh dannykh» (ID proekta 02/08/03-25/00155867 ot 27.03.2025) (In Russ.)]
 30. Приказ Минздрава России от 14.06.2018 №341н «Об утверждении Порядка обезличивания сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования». [Prikaz Minzdrava Rossii ot 14.06.2018 №341n «Ob utverzhdenii Poryadka obezlichivaniya svedenij o licakh, kotorym okazyvaetsya medicinskaya pomoshch', a takzhe o licakh,

- v otnoshenii kotorykh provodyatsya medicinskie ehkspertizy, medicinskie osmotry i medicinskie osviditel'stvovaniya». (In Russ.)]
31. Постановление Правительства Российской Федерации от 09.02.2022 №140 «О единой государственной информационной системе в сфере здравоохранения». [Postanovlenie Pravitel'stva Rossijskoj Federacii ot 09.02.2022 №140 «O edinoj gosudarstvennoj informacionnoj sisteme v sfere zdravookhraneniya». (In Russ.)]
 32. Приказ Минздрава России от 20.03.2025 №139н «Об утверждении Порядка обезличивания сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования». [Prikaz Minzdrava Rossii ot 20.03.2025 №139n «Ob utverzhdenii Poryadka obezlichivaniya svedenij o licakh, kotorym okazyvaetsya medicinskaya pomoshch', a takzhe o licakh, v otnoshenii kotorykh provodyatsya medicinskie ehkspertizy, medicinskie osmotry i medicinskie osviditel'stvovaniya». (In Russ.)]
 33. Борисов А.В., Босов А.В., Иванов А.В. Применение имитационного компьютерного моделирования к задаче обезличивания персональных данных. Оценка состояния и основные положения // Программирование. — 2023. — №4. — С.58-74. [Borisov SA, Bosov AA, Ivanov DE. Application of Simulated Computer Modeling to the Problem of Depersonalization of Personal Data. Condition Assessment and Key Poins. Programming. 2023; 4: 58-74 (In Russ.)] doi: 10.31857/s0132347423040040.
 34. Мищенко Е.Ю., Соколов А.Н. Количественные критерии идентификации физического лица при обезличивании персональных данных // Вестник УрФО. Безопасность в информационной сфере. — 2014. — №1(11). — С.27-33. [Mishchenko EYu, Sokolov AN. Quantitative analysis of the Depersonalization Procedure. Method of Identifiers. Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics. 2015; 15(3): 18-25. (In Russ.)] doi: 10.14529/ctcr150303.
 35. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. Доступно по: <https://docs.cntd.ru/document/1200095035>. Ссылка действительна на 10.05.2025. [GOST R 34.11-2012. Information technology. Cryptographic data security. Hash-function. Available at: <https://docs.cntd.ru/document/1200095035>. Accessed 10.05.2025. (In Russ.)]
 36. Федеральный закон «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации» от 08.06.2020 №168-ФЗ. [Federal'nyj zakon «O edinom federal'nom informacionnom registre, soderzhashchem svedeniya o naselenii Rossijskoj Federacii» ot 08.06.2020 №168-FZ. (In Russ.)]
 37. Постановление Правительства Российской Федерации от 09.10.2021 №1723 «Об утверждении Правил предоставления сведений, содержащихся в едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации, в том числе перечня указанных сведений и сроков их предоставления, и перечня обезличенных персональных данных, содержащихся в едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации». [Postanovlenie Pravitel'stva Rossijskoj Federacii ot 09.10.2021 №1723 «Ob utverzhdenii Pravil predostavleniya svedenij, soderzhashchikhsya v edinom federal'nom informacionnom registre, soderzhashchem svedeniya o naselenii Rossijskoj Federacii, v tom chisle perechnya ukazannykh svedenij i srokov ikh predostavleniya, i perechnya obezlichennykh personal'nykh dannykh, soderzhashchikhsya v edinom federal'nom informacionnom registre, soderzhashchem svedeniya o naselenii Rossijskoj Federacii». (In Russ.)]
 38. Постановление Правительства Российской Федерации от 05.02.2022 №116 «Об утверждении Правил ведения Федерального реестра медицинских документов о рождении». [Postanovlenie Pravitel'stva Rossijskoj Federacii ot 05.02.2022 №116 «Ob utverzhdenii Pravil vedeniya Federal'nogo reestra medicinskikh dokumentov o rozhdenii». (In Russ.)]
 39. Приказ Минздрава России от 13.10.2021 №987н «Об утверждении формы документа о рождении и порядка его выдачи». [Prikaz Minzdrava Rossii ot 13.10.2021 №987n «Ob utverzhdenii formy dokumenta o rozhdenii i poryadka ego vydachi». (In Russ.)]

40. Марцевич С.Ю., Кутишенко Н.П., Лукина Ю.В., Лукьянов М.М., Драпкина О.М. Наблюдательные исследования и регистры. Их качество и роль в современной доказательной медицине. Кардиоваскулярная терапия и профилактика. — 2021. — №20(2). — С.2786. [Martsevich SYu, Kutishenko NP, Lukina YuV, Lukyanov MM, Drapkina OM. Observational studies and registers. Their quality and role in modern evidencebased medicine. Cardiovascular Therapy and Prevention. 2021; 20(2): 2786. (In Russ.)] doi: 10.15829/1728-8800-2021-2786.
41. Иванов А.В. Регистры как основа для сбора данных и построения доказательств // Реальная клиническая практика: данные и доказательства. — 2021. — №1(1). — С.10-15. [Ivanov AV. Registers as a basis for data collection and evidence building. Real-World Data & Evidence. 2021; 1(1): 10-15. (In Russ.)] doi: 10.37489/2782-3784-myrd-3.
42. Марцевич С.Ю., Лукина Ю.В., Кутишенко Н.П., Толпыгина С.Н., Лукьянов М.М., Драпкина О.М. Медицинские регистры. Роль в доказательной медицине. Рекомендации по созданию. Методические рекомендации. — М.: ФГБУ «НМИЦ ТПМ» Минздрава России, 2023. — 44 с. [Martsevich SYu, Lukina YuV, Kutishenko NP, Tolpygina SN, Lukyanov MM, Drapkina OM. Medical registers. Role in evidence-based medicine. Recommendations for creation. Methodological recommendations. M.: FGBU «NMIC TPM» of the Ministry of Health of Russia. 2023. 44 pp. (In Russ.)] doi: 10.15829/ROPNIZ-m1-2023.
43. Единый план по достижению национальных целей развития Российской Федерации до 2030 года и на перспективу до 2036 года. Утвержден Правительством Российской Федерации 09.01.2025. [Edinyj plan po dostizheniyu nacional'nykh celej razvitiya Rossijskoj Federacii do 2030 goda i na perspektivu do 2036 goda. Utverzhden Pravitel'stvom Rossijskoj Federacii 09.01.2025. (In Russ.)]
44. Gavrilo D, Gusev A, Korsakov I, Novitsky R, Serova L. Feature Extraction Method from Electronic Health Records in Russia, in Proceedings of the FRUCT'26. pp. 497-500. April 2020.
45. Макарова Е.А., Андрейченко А.Е., Казакова М.А., Иванов Д.А., Гусев А.В. Обезличивание медицинских текстовых данных с целью разработки и внедрения систем искусственного интеллекта // Правовая информатика. — 2024. — №3. — С.96-105. [Makarova E., Andreichenko A., Kazakova M, Ivanov D, Gusev A. Depersonalisation of Medical text data with a view to developing and implementing artificial intelligence systems. Legal Informatics. 2024; 3: 96-105. (In Russ.)] doi: 10.24682/1994-1404-2024-3-96-105.

46. ГОСТ Р ИСО 22077-1-2017. Информатизация здоровья. Формат биосигналов. Часть 1. Правила кодирования. Доступно по: <https://docs.cntd.ru/document/1200146051>. Ссылка действительна на 10.05.2025. [GOST R ISO 22077-1-2017 Health informatics. Medical waveform format. Part 1. Encoding rules. Available at: <https://docs.cntd.ru/document/1200146051>. Accessed 10.05.2025. (In Russ.)]
47. ГОСТ Р ИСО 11073-91064-2017. Информатизация здоровья. Стандартный протокол коммуникаций. Часть 91064. Компьютерная электрокардиография. Доступно по: <https://docs.cntd.ru/document/1200147099>. Ссылка действительна на 10.05.2025. [GOST R ISO 22077-91064-2017. Health Informatics. Standard communication protocol. Part 91064. Computer-assisted electrocardiography. Available at: <https://docs.cntd.ru/document/1200147099>. Accessed 10.05.2025. (In Russ.)]
48. ГОСТ Р ИСО/МЭК 27038-2016. Информационные технологии. Методы обеспечения безопасности. Требования и методы электронного цензурирования. Доступно по: <https://docs.cntd.ru/document/1200136904>. Ссылка действительна на 10.05.2025. [GOST R ISO/IEC 27038-2016. Information technologies. Security techniques. Specification for digital redaction. Available at: <https://docs.cntd.ru/document/1200136904>. Accessed 10.05.2025. (In Russ.)]
49. ГОСТ Р 71674-2024. Системы искусственного интеллекта в клинической медицине. Набор данных в формате DICOM для тестирования алгоритмов. Методы обезличивания набора данных и контроля набора данных на отсутствие персональных данных. Доступно по: <https://docs.cntd.ru/document/1309958855>. Ссылка действительна на 10.05.2025. [GOST R 71674-2024. Artificial intelligence in routine clinical practice. DICOM dataset for algorithm testing. Dataset de-identification and monitoring for presence of personal data. Available at: <https://docs.cntd.ru/document/1309958855>. Accessed 10.05.2025. (In Russ.)]
50. Борисов А.В., Босов А.В., Иванов А.В. Применение имитационного компьютерного моделирования к задаче обезличивания персональных данных. Модель и алгоритм обезличивания методом синтеза // Программирование. — 2023. — №5. — С.19-34. [Borisov SA, Bosov AA, Ivanov DE. Application of Simulated Computer Modeling to the Problem of Depersonalization of Personal Data. Model and Algorithm for decontamination by synthesis. Programming. 2023; 5: 19-34. (In Russ.)] doi: 10.31857/s0132347423050023.