УТВЕРЖДАЮ
Руководитель Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций
_____ А.А. Жаров
«13» _____12_____ 2013 г.

Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»

Общие положения

Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 утвержден перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами (далее – Перечень).

В соответствии с п.п. з) п. 1 Перечня одной из мер, направленных, в первую очередь, на минимизацию рисков причинения вреда конкретным гражданам в случае утечки их персональных данных из информационных систем персональных данных, является обезличивание персональных данных согласно требованиям и методам, установленным уполномоченным органом по защите прав субъектов персональных данных.

Роскомнадзором, как уполномоченным органом по защите прав субъектов персональных данных в Российской Федерации, установлены требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, которые утверждены приказом Роскомнадзора от 5 сентября 2013 г. № 996 (далее – Приказ).

Данные методические рекомендации разработаны с целью оказания помощи операторам, осуществляющим обработку персональных данных и являющимся государственными или муниципальными органами (далее – Методические рекомендации, Операторы), в выборе предпочтительных вариантов реализации утвержденных требований и методов на практике.

Методические рекомендации содержат методологию обезличивания персональных данных в информационных системах, а также построение процессов

дальнейшей обработки данных, полученных в результате обезличивания (далее – обезличенные данные).

Методические рекомендации содержат анализ процессов автоматизированной обработки обезличенных данных, требований к обезличенным данным и методам обезличивания, позволяющий выделить основные свойства обезличенных данных и методов обезличивания и оценить возможности их применения при решении задач обработки персональных данных с учетом вида деятельности Оператора и необходимых действий с персональными данными.

В Методических рекомендациях используются следующие термины и определения:

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Деобезличивание – действия, в результате которых обезличенные данные принимают вид, позволяющий определить их принадлежность конкретному субъекту персональных данных, то есть становятся персональными данными.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обезличенные данные – это данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному субъекту персональных данных невозможно определить без дополнительной информации.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Обработка обезличенных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации, с обезличенными данными, без применения их предварительного деобезличивания.

Оператор – государственный орган или муниципальный орган, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) и хранимая в информационных системах в электронном виде.

Персональные данные субъекта представляются в виде записи, которая является самостоятельной единицей данных, имеет определенную структуру и содержит множество значений атрибутов персональных данных субъекта.

Обезличенные данные субъекта представляются в виде записи, которая является самостоятельной единицей данных, имеет определенную структуру и содержит множество значений атрибутов обезличенных данных.

Атрибут персональных данных субъекта – элемент структуры персональных данных (параметр персональных данных). Атрибут имеет название и может иметь множество возможных количественных и качественных значений применительно к конкретным субъектам персональных данных.

Атрибут обезличенных данных субъекта – элемент структуры обезличенных данных (параметр обезличенных данных). Атрибут имеет название и может иметь множество возможных количественных и качественных значений.

Семантика атрибута персональных данных – смысловое значение названия атрибута, обозначения персональных данных.

Семантика атрибута, обезличенных данных – смысловое значение названия атрибута, обозначения обезличенных данных.

Персональные данные множества субъектов представлены в виде множества (массива) записей персональных данных.

Ниже приводятся свойства обезличенных персональных данных, определяющие возможность их применения для конкретных видов обработки персональных данных с целью решения прикладных задач, стоящих перед Оператором в зависимости от вида его деятельности, и связанных с обработкой персональных данных.

Свойства обезличенных данных:

Полнота – сохранение всей информации о персональных данных конкретных субъектов или группах субъектов, которая имелась до обезличивания.

Структурированность – сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания.

Релевантность – возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме.

Семантическая целостность – соответствие семантики атрибутов обезличенных данных семантике соответствующих атрибутов персональных данных при их обезличивании.

Применимость – возможность обработки персональных данных с целью решения задач, стоящих перед Оператором, без предварительного деобезличивания всего объема записей о субъектах.

Анонимность – невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации.

Наличие перечисленных свойств обеспечивается применяемыми методами обезличивания.

1. Методы обезличивания

Методы обезличивания, кроме обеспечения требуемых свойств обезличенных данных, должны быть практически реализуемыми в различных программных средах и позволять решать поставленные перед Оператором задачи обработки персональных данных либо с предварительным деобезличиванием, либо без деобезличивания.

К методам обезличивания, установленным Приказом, относятся:

метод введения идентификаторов – замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным;

метод изменения состава или семантики – изменение состава или семантики персональных данных путем замены результатами статистической обработки, преобразования, обобщения или удаления части сведений;

метод декомпозиции – разделение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;

метод перемешивания – перестановка отдельных значений или групп значений атрибутов персональных данных в массиве персональных данных.

Применение того или иного метода обезличивания позволит получить обезличенные данные, обладающие различными свойствами, что даст возможность осуществлять все виды обработки персональных данных. В связи с этим, в описании методов обезличивания указаны условия, обеспечивающие выполнение определенных свойств и требований.

Следует также отметить, что существуют виды (задачи) обработки персональных данных, когда наличие всех требуемых свойств не обязательно, например, при решении статистических задач. Таким образом, в каждом конкретном случае необходимо применять метод, который гарантирует свойства, необходимые для решения конкретных задач обработки стоящих перед Оператором.

Далее, в описании методов обезличивания, приводятся рекомендации по применению утвержденных методов обезличивания.

1.1. Метод введения идентификаторов.

Метод реализуется путем замены части персональных данных, позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия (справочника идентификаторов).

Применение данного метода позволяет получить обезличенные данные обладающие следующими свойствами:

полнота – информация, позволяющая идентифицировать субъектов персональных данных, не удаляется, а переносится в таблицу соответствия;

структурированность – каждому идентификатору после процедуры обезличивания однозначно соответствует свой набор данных;

семантическая целостность – вид представления данных не меняется, они лишь переносятся в таблицу соответствия.

Анонимность возможно обеспечить только при определенных правилах выбора идентификаторов и заменяемых ими персональных данных, поскольку метод не устойчив к атакам, направленным на справочники идентификаторов при косвенном деобезличивании и атакам, направленным на деобезличивание с использованием информации из справочников идентификаторов, кроме того, стойкость метода не повышается с увеличением объема обезличиваемых данных.

Также обеспечивается применимость - Оператор может осуществлять обработку отдельных записей и всех обезличенных данных без деобезличивания.

Обезличенные данные, полученные в результате применения названного метода, не будут обладать свойством релевантности, поскольку в запросе и в ответе на запрос изменяется вид представления персональных данных, которые были заменены идентификаторами.

Применение данного метода позволит сохранить в записях связи между атрибутами обезличенных данных, соответствующие связям между атрибутами персональных данных.

Метод введения идентификаторов целесообразно применять при небольшом количестве атрибутов персональных данных и небольшом объеме массива персональных данных, в связи с тем, что объем справочников будет напрямую зависеть от этих параметров. Вычислительная эффективность метода значительно снижается при частом внесении изменений в состав данных и значения атрибутов.

1.2. Метод изменения состава или семантики.

Метод реализуется путем обобщения, изменения значений атрибутов персональных данных или удаления части сведений, позволяющих идентифицировать субъекта.

Применение данного метода позволяет получить обезличенные данные, обладающие следующими свойствами:

структурированность - связь между отдельными значениями атрибутов персональных данных субъекта не нарушается;

анонимность – удаление или обобщение части данных приводит к неоднозначности при идентификации с использованием обезличенных данных.

Полученные обезличенные данные могут обладать свойством полноты только при проведении изменений в составе персональных данных, гарантирующих сохранность данных. При удалении части сведений, полученные обезличенные данные утрачивают свойство полноты.

Семантическая целостность полученных данных обеспечивается только при условии проведения изменений в составе персональных данных, сохраняющих семантику данных. Изменения должны учитывать специфику задач обработки, стоящих перед Оператором.

Также обеспечиваются следующие свойства обезличенных данных:

частичная релевантность, поскольку в определенных случаях возможно получить семантическое соответствие поискового запроса и полученного ответа на запрос;

применимость, поскольку Оператор может осуществлять обработку, не требующую деобезличивания всего объема данных о субъектах.

При выделении атрибутов персональных данных необходимо учитывать возможность проведения обезличивания с использованием данных атрибутов. При простом изменении значений отдельных атрибутов обезличивание может не произойти, поскольку произойдет только изменение состава персональных данных.

Применение данного метода позволяет частично сохранить в записях связи между атрибутами обезличенных данных, соответствующие связям между атрибутами персональных данных.

Метод изменения состава и семантики целесообразно применять в случае, когда возможно изменение состава и семантики, так, что задачи обработки персональных данных не требуют деобезличивания, поскольку метод не обладает свойством обратимости при любых изменениях состава и семантики данных. В противном случае необходимо использовать дополнительную информацию для проведения деобезличивания.

Данный метод также целесообразно применять в случаях автономного использования Оператором обезличенных данных, когда не требуется совместимость с данными других Операторов.

1.3. Метод декомпозиции.

Метод реализуется путем разделения множества атрибутов персональных данных на несколько подмножеств и создания таблиц, устанавливающих связи между подмножествами (таблицы связей), с последующим раздельным хранением записей, соответствующих подмножествам этих атрибутов.

Применение данного метода позволит получить обезличенные данные, обладающие следующими свойствами:

полнота - информация о субъектах персональных данных не удаляется, а переносится в другое хранилище;

структурированность - сохраняется связь между записями в разных хранилищах, что позволяет однозначно сопоставлять их;

семантическая целостность – семантика и вид представления данных о субъекте не изменяется.

Анонимность обеспечивается только при достаточно сложных связях между хранилищами и защите хранилищ от несанкционированного доступа, поскольку метод не устойчив к атакам, направленным на деобезличивание путем анализа данных из различных хранилищ и косвенному деобезличиванию.

Также обеспечиваются следующие свойства обезличенных данных:

релевантность, поскольку возможно получить семантическое соответствие поискового запроса и полученного ответа на запрос;

применимость, поскольку Оператор может осуществлять обработку данных, расположенных в одном хранилище, как независимо от другого, так и при

совместном их использовании, без деобезличивания всего объема обезличенных данных.

Применение данного метода позволяет сохранить в записях каждого хранилища связи между атрибутами обезличенных данных, соответствующие связям между атрибутами персональных данных.

Метод декомпозиции целесообразно применять при большом количестве атрибутов персональных данных, но при достаточно редком внесении изменений в состав данных и значения атрибутов.

1.4. Метод перемешивания.

Метод реализуется путем перемешивания (перестановки) отдельных значений или групп значений атрибутов персональных данных между собой.

Применение данного метода позволит получить обезличенные данные, обладающие следующими свойствами:

полнота – вся информация о субъектах персональных данных сохраняется;

структурированность - связи между данными полностью восстанавливаются при деобезличивании;

семантическая целостность – семантика и вид представления данных о субъекте не изменяется;

анонимность - данные перемешиваются по каждому отдельному атрибуту записи о субъекте, что не позволяет без доступа к дополнительной (служебной) информации определить принадлежность тех или иных данных конкретному субъекту.

Также обеспечиваются следующие свойства обезличенных данных:

релевантность, поскольку возможно получить семантическое соответствие поискового запроса и полученного ответа на запрос;

применимость, поскольку при наличии доступа к дополнительной (служебной) информации Оператор может осуществлять обработку как отдельных записей о субъектах, так и всех данных, без деобезличивания всего объема обезличенных данных.

Применение данного метода не позволяет сохранить в записях связи между атрибутами обезличенных данных, соответствующие связям между атрибутами персональных данных.

Метод перемешивания целесообразно применять при большом количестве атрибутов персональных данных и большом объеме массива персональных данных, поскольку стойкость метода к атакам направленным на деобезличивание увеличивается с увеличением указанных параметров, а количество дополнительной информации слабо зависит от объема массива персональных данных.

Метод перемешивания эффективен при необходимости сложной обработки персональных данных, частом внесении изменений в значения атрибутов.

Результаты сопоставления свойства обезличенных данных с методами обезличивания приведены в Таблице 1.

Таблица 1 – Соответствие методов обезличивания свойствам обезличенных данных

Метод обезличивания / Свойства обезличенных данных	Метод введения идентификаторов	Метод изменения состава или семантики	Метод декомпозиции	Метод перемешивания
Полнота	+	+/-	+	+
Структурированность	+	+	+	+
Релевантность	+/-	+	+	+
Семантическая целостность	+	+/–	+	+
Применимость	+	+	+	+
Анонимность	+/-	+	+/-	+
+ безусловное наличие свойства +/- условное наличие свойства, см. описание метода				

2. Процедуры обезличивания

Процедура обезличивания обеспечивает практическую реализацию метода обезличивания и задается своим описанием.

Допускается программная реализация процедуры различными способами и средствами, доступными Оператору.

Различные способы реализации одной процедуры должны обеспечивать одинаковые результаты.

Описание процедуры обезличивания должно обеспечивать однозначную трактовку проводимых действий по обезличиванию/деобезличиванию и включает:

алгоритмы обезличивания и деобезличивания;

параметры процедур обезличивания/деобезличивания;

оценку объема дополнительных данных (параметры процедуры) для проведения обезличивания;

правила проведения процедуры и выбора значений параметров процедуры;

характеристики процедуры, связанные с качеством обезличенных данных, ее трудоемкостью, стойкость к различным атакам.

2.1. Процедура реализации метода введения идентификаторов

Каждому значению идентификатора должно соответствовать одно значение атрибута и каждому значению атрибута должно соответствовать одно значение идентификатора.

Таблицы соответствия (дополнительные данные) создаются для каждого атрибута персональных данных, значения которых заменяются идентификаторами.

При обезличивании персональные данные в исходном множестве заменяются идентификаторами согласно таблице соответствия. Деобезличивание достигается обратной заменой идентификаторов на значения персональных данных по таблице соответствия.

На этапе реализации процедуры обезличивания определяются следующие параметры:

перечень таблиц соответствия (перечень атрибутов, для которых происходит замена значений идентификаторами);

правила вычисления идентификаторов – наборов символов, однозначно соответствующих значениям атрибутов персональных данных субъекта;

объемы таблицы соответствия – количество строк таблицы соответствия, содержащих идентификатор и соответствующее ему значение.

В качестве атрибутов, значения которых заменяются идентификаторами, как правило, выбираются атрибуты, однозначно идентифицирующие субъекта персональных данных.

Количество идентификаторов и объем таблиц соответствия, как правило, равны исходному количеству субъектов персональных данных. Возможны случаи, когда идентификатор вычисляется в зависимости от значения соответствующего атрибута.

Таблицы соответствия должны быть доступны ограниченному числу сотрудников Оператора.

Программное обеспечение, реализующее процедуру, должно обеспечивать внесение изменений и поддержку актуальности таблиц соответствия.

2.2. Процедура реализации метода изменения состава или семантики

Процедура реализации метода должна содержать правила удаления либо замены значений персональных данных субъектов на новые значения, вычисляемые по заданным правилам.

При замене значений атрибутов на новые, требуется устанавливать правила обратной замены если это необходимо для деобезличивания.

На этапе реализации процедуры обезличивания необходимо определить следующие параметры:

перечень атрибутов персональных данных, подлежащих удалению;

перечень атрибутов персональных данных, подлежащих замене на новые значения;

правила вычисления значений для замены (обратной замены) персональных данных субъектов.

Программная реализация процедуры должна обеспечить возможность внесения изменений и дополнений в состав обезличенных данных, динамическое вычисление значений для замены при занесении новых субъектов, проверку и поддержку актуальности данных.

2.3. Процедура реализации метода декомпозиции

Процедура реализации метода по заданному правилу (алгоритму) производит разделение исходного массива персональных данных на несколько частей, каждая из которых содержит заданный набор атрибутов всех субъектов. Сведения, содержащиеся в каждой части, не позволяют идентифицировать субъектов персональных данных.

Деобезличивание осуществляется по заданному набору связей (используются таблицы связей, являющиеся дополнительными данными) между раздельно хранимыми частями.

На этапе реализации процедуры обезличивания необходимо определить следующие параметры:

перечень атрибутов, составляющих подмножества персональных данных;

таблицы связей между подмножествами персональных данных;

адреса хранения подмножеств персональных данных.

Правила разделения исходного массива данных определяются таким образом, чтобы каждая из раздельно хранимых частей не содержала сведений, позволяющих однозначно идентифицировать субъекта персональных данных.

Программная реализация процедуры должна обеспечивать согласованное внесение изменений и дополнений во все подмножества и таблицы связей, поиск данных о субъекте во всех подмножествах, поддержку актуальности таблиц связей, проверку полноты данных (согласование подмножеств).

2.4. Процедура реализации метода перемешивания

Метод перемешивания реализуется путем перемешивания отдельных значений или групп значений атрибутов субъектов персональных данных между собой.

Перемешивание проводится по установленному правилу.

Деобезличивание достигается с использованием процедуры, обратной процедуре перемешивания.

Для реализации процедуры необходимо определить алгоритм перемешивания и его параметры.

На этапе реализации процедуры обезличивания необходимо определить следующие параметры:

набор параметров алгоритма перемешивания (дополнительные данные для обезличивания/деобезличивания);

значения параметров алгоритма перемешивания (дополнительные данные для обезличивания/деобезличивания).

Выбор параметров перемешивания зависит от алгоритма перемешивания, требуемой стойкости к атакам, и объема обезличиваемых персональных данных.

Программная реализация процедуры должна обеспечивать возможность внесения изменений и дополнений в состав обезличенных данных, добавление новых пользователей, поддержку актуальности данных и возможность повторного перемешивания с новыми параметрами без предварительного деобезличивания.

3. Организация обработки обезличенных данных

При использовании Оператором процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

Обезличивание персональных данных субъектов должно производиться Оператором перед внесением их в информационную систему.

Оператор вправе обрабатывать в информационной системе обезличенные данные, полученные от третьих лиц.

В процессе обработки обезличенных данных Оператором, при необходимости, может проводиться деобезличивание. После обработки персональные данные, полученные в результате такого деобезличивания уничтожаются.

Обработка персональных данных до осуществления процедур обезличивания и после выполнения операций деобезличивания должна осуществляться в соответствии с действующим законодательством Российской Федерации с применением мер по обеспечению безопасности персональных данных.

Обработка обезличенных данных должна осуществляться с использованием технических и программных средств, соответствующих форме представления и хранения данных.

Обработка персональных данных организаций, не обладающих квалифицированным персоналом либо достаточными материально-техническими средствами, возможна с привлечением сторонних организаций - Операторов на основании договора. При использовании технологий «облачной» обработки персональных данных возможна обработка одним Оператором обезличенных данных нескольких подобных организаций.

При обработке обезличенных данных необходимо выделять зоны ответственности Операторов, субъектов и/или организаций, поручивших обработку Оператору.

Алгоритмы для реализации процедур обезличивания и программное обеспечение должны обеспечивать переносимость на различные аппаратные платформы.

Действия, связанные с внесением изменений и дополнений в массив обезличенных данных следует проводить в режиме транзакций и отражать в соответствующем журнале.

Следует вести архив запросов на обработку данных.

Субъект персональных данных должен иметь возможность получить сведения о составе его персональных данных, имеющихся у Оператора.

Хранение и защиту дополнительной (служебной) информации, содержащей параметры методов и процедур обезличивания/деобезличивания, следует обеспечить в соответствии с внутренними процедурами обеспечения конфиденциальности, установленными у Оператора. При этом должно обеспечиваться исполнение установленных правил доступа пользователей к хранимым данным, резервного копирования и возможности актуализации и восстановления хранимых данных.

Процедуры обезличивания/деобезличивания должны встраиваться в процессы обработки персональных данных как их неотъемлемый элемент, а также

максимально эффективно использовать имеющуюся у Оператора инфраструктуру, обеспечивающую обработку персональных данных.

Оператору рекомендуется разработать и применять при осуществлении своей деятельности документацию, включающую:

описание применяемых процедур и их программного обеспечения;

инструкции по проведению процедур обезличивания/деобезличивания;

инструкции по обработке обезличенных данных;

инструкции проведения контроля качества обезличенных данных и процедур обезличивания;

порядок взаимодействия с другими Операторами;

инструкции по обеспечению безопасности дополнительной (служебной) информации, содержащей параметры методов и процедур обезличивания/деобезличивания;

техническую и эксплуатационную документацию, поставляемую с программными средствами, обезличивания/деобезличивания.

4. Правила работы Операторов с обезличенными данными

Оператору следует:

обеспечить соответствие процедур обезличивания/деобезличивания персональных данных требованиям к обезличенным данным и методам обезличивания;

обеспечить соответствие процедур обезличивания/деобезличивания условиям и целям обработки персональных данных;

убедиться, что при реализации процедур обезличивания/ деобезличивания, а так же при последующей обработке обезличенных данных не нарушаются права субъекта персональных данных.

В случае, когда обработка обезличенных данных была поручена Оператору третьим лицом, Оператору следует соблюдать все требования, предъявляемые этим лицом.

В процессе реализации процедуры обезличивания персональных данных Оператору следует соблюдать все регламентные требования, предъявляемые к выбранному способу реализации процедуры обезличивания.

При хранении обезличенных данных Оператору следует:

организовать раздельное хранение обезличенных данных и дополнительной (служебной) информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания;

обеспечивать конфиденциальность дополнительной (служебной) информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания.

При передаче вместе с обезличенными данными информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания Оператору следует обеспечить конфиденциальность канала (способа) передачи данных.

В ходе реализации процедуры деобезличивания Оператору следует:

реализовать все требования по обеспечению безопасности получаемых персональных данных при автоматизированной обработке на средствах вычислительной техники, участвующих в реализации процедуры деобезличивания и обработке деобезличенных данных;

обеспечить обработку и защиту деобезличенных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

5. Рекомендации по выбору методов и процедур обезличивания персональных данных

5.1. Методология выбора методов и процедур обезличивания

При выборе методов и процедур обезличивания персональных данных Оператору следует руководствоваться целями и задачами обработки персональных данных.

Обезличивание персональных данных, обработка которых осуществляется с разными целями, может осуществляться разными методами.

Возможно объединение различных методов обезличивания в одну процедуру.

Для решения каждой задачи обработки Оператор определяет требуемые свойства обезличенных данных и метода обезличивания, которые зависят от набора действий, осуществляемых Оператором с персональными данными (сбор, хранение, изменение, систематизация, осуществление выборки, поиск, передача и т.д.) в соответствии с принципом разумной достаточности (определяется минимально необходимый перечень свойств). Целесообразно предусмотреть возможность обработки обезличенных данных без предварительного деобезличивания.

При выборе метода и процедуры обезличивания так же следует учитывать:

объем персональных данных, подлежащих обезличиванию (некоторые методы неэффективны на малых объемах);

форму представления данных (отдельные записи, файлы, таблицы баз данных и т.д.);

область обработки обезличенных данных (необходим ли другим Операторам доступ к обезличиваемым данным);

способы хранения обезличенных данных (локальное хранение, распределенное хранение и т.д.);

применяемые в информационной системе Оператора меры по обеспечению безопасности данных.

5.2. Рекомендации по выбору методов обезличивания в соответствии с классом задач обработки

Ниже представлены типовые классы задач, состоящие из наиболее часто встречающихся задач обработки персональных данных в государственных и муниципальных органах. Проведенная классификация позволяет Оператору применять наиболее эффективные для данного класса методы.

В Таблице 2 приведены рекомендации по выбору метода обезличивания в зависимости от класса решаемых задач. Рекомендованные методы ранжированы в порядке убывания эффективности их применения.

Таблица 2 – Сопоставление задач обработки методам обезличивания

Класс задач	Задачи обработки	Метод обезличивания
Статистическая обработка и статистические исследования ПД	- осуществление выборки по заявленным параметрам; - проведение исследований по заданным параметрам субъектов.	- метод перемешивания; - метод декомпозиции; - метод изменения состава или семантики.
Сбор и хранение	- внесение персональных	- метод декомпозиции;

ПД	данных субъектов в информационную систему на основе анкет, заявлений и прочих документов.	- метод перемешивания; - метод введения идентификаторов.
Обработка поисковых запросов (поиск данных о субъектах и поиск субъектов по известным данным)	- поиск информации о субъектах; - печать и выдача субъектам документов в установленной форме, содержащих персональные данные; - выдача справок, выписок, уведомлений по запросам субъектов или уполномоченных органов.	- метод перемешивания; - метод декомпозиции; - метод введения идентификаторов.
Актуализация ПД	- внесение изменений в существующие записи о субъектах на основе обращений субъектов, решений судов и других уполномоченных органов; - внесение изменений в существующие записи о субъектах на основе исследований, выполнения органом своих функций или требований законодательства РФ.	- метод перемешивания; - метод декомпозиции; - метод введения идентификаторов.
Интеграция данных различных Операторов	- поиск информации о субъектах; - передача данных смежным органам.	- метод перемешивания; - метод декомпозиции; - метод введения идентификаторов.
Ведение учета субъектов ПД	- прием анкет, заявлений; - ведение учета персональных данных в соответствии с функциями органа.	- метод декомпозиции; - метод перемешивания; - метод введения идентификаторов.

При наличии в системе нескольких классов задач рекомендуется выбирать общий метод для всех этих классов, либо совместно применять несколько методов.

Практическая реализация методов и обработка обезличенных данных может проводиться с применением различных информационных технологий.

В Таблице 3 приведены рекомендации по выбору типа технологии обработки обезличенных данных.

Методы ранжированы в порядке их предпочтительности.

При составлении таблицы учитывались возможности обеспечения безопасности данных.

Таблица 3 – Типы технологий обработки обезличенных данных

Технология	Метод обезличивания
Клиент – сервер с использованием серверов Оператора	- метод перемешивания; - метод декомпозиции; - метод введения идентификаторов.
Распределенная обработка на нескольких удаленных серверах (объектные вычисления)	- метод перемешивания; - метод декомпозиции; - метод введения идентификаторов.
Центры обработки данных	- метод перемешивания; - метод декомпозиции; - метод введения идентификаторов.
Облачные вычисления	- метод перемешивания; - метод декомпозиции; - метод введения идентификаторов.

Примеры реализации методов обезличивания

Исходный вид таблицы персональных данных:

ФИО	Дата рождения	Адрес проживания	Номер телефона	
Иванов Иван Иванович	01.02.1970	г. Москва, ул. Тверская, д.1, кв. 1.	+7 495-111-1111	Сердечная не
Петров Петр Петрович	02.03.1975	г. Самара, ул. Ленина, д.2, кв. 2.	+7 846-121-2311	ВИЧ
Сидоров Иван Петрович	03.04.1970	г. Москва, ул. Кутузова, д.3, кв. 3.	+7 495-222-1111	Хронические

А.1. Применение метода введения идентификаторов

Таблица обезличенных данных (Атрибут *ФИО* заменен на идентификатор)

Идентификатор	Дата рождения	Адрес проживания	Номер телефона	
АА12345	01.02.1970	г. Москва, ул. Тверская, д.1, кв. 1.	+7 495-111-1111	Сердечная не
ББ23456	02.03.1975	г. Самара, ул. Ленина, д.2, кв. 2.	+7 846-121-2311	ВИЧ
ВВ34567	03.04.1970	г. Москва, ул. Кутузова, д.3, кв. 3.	+7 495-222-1111	Хронические

Таблица идентификаторов

Идентификатор	ФИО
АА12345	Иванов Иван Иванович
ББ23456	Петров Петр Петрович
ВВ34567	Сидоров Иван Петрович

А.2. Применение метода изменения состава или семантики

Дата рождения	Адрес проживания	Диагноз
01.02.1970	г. Москва	Сердечная недостаточность
02.03.1975	г. Самара	ВИЧ
03.04.1970	г. Москва	Хронический мигрени

Атрибуты *ФИО* и *Номер телефона* были удалены. Атрибут *Адрес проживания* был обобщен до горо

А.3. Применение метода декомпозиции

Исходная таблица персональных данных разбивается на две таблицы, хранимые раздельно.

Таблица 1.

№	ФИО	Дата рождения
1	Иванов Иван Иванович	01.02.1970
2	Петров Петр Петрович	02.03.1975
3	Сидоров Иван Петрович	03.04.1970

Таблица 2.

№	Адрес проживания	Номер телефона
1	г. Москва, ул. Тверская, д.1, кв. 1.	+7 495-111-1111
2	г. Самара, ул. Ленина, д.2, кв. 2.	+7 846-121-2311
3	г. Москва, ул. Кутузова, д.3, кв. 3.	+7 495-222-1111

Таблица 3 (Таблица связей между Таблицей 1 и Таблицей 2)

№	Номер строки Таблицы 1	Номер строки Таблицы 2
1	1	1
2	2	2
3	3	3

А.4. Применение метода перемешивания

Таблица обезличенных данных

№	ФИО	Дата рождения	Адрес проживания	Номер телефона	
1	Сидоров Иван Петрович	02.03.1975	г. Москва, ул. Тверская, д.1, кв. 1.	+7 495-222-1111	Серде
2	Петров Петр Петрович	01.02.1970	г. Самара, ул. Ленина, д.2, кв. 2.	+7 495-111-1111	ВИЧ
3	Иванов Иван Иванович	03.04.1970	г. Москва, ул. Кутузова, д.3, кв. 3.	+7 846-121-2311	Хрон