Приложение № 6 к приказу «Об обеспечении безопасности персональных данных в ГБОУВО РК КИПУ имени Февзи Якубова»
от 05.09.2023 г. № 449

Правила
обезличивания персональных данных и работы с ними в ГБОУВО РК КИПУ имени Февзи Якубова

1. Общие положения

1.1. Настоящие Правила обезличивания персональных данных и работы с ними в ГБОУВО РК КИПУ имени Февзи Якубова (далее соответственно – Правила, Университет) включают в себя описание методов обезличивания персональных данных (далее – ПДн), процедур обезличивания ПДн, организации обработки обезличенных ПДн, правил работы с обезличенными ПДн, выбор методов и процедур обезличивания ПДн в Университете.

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

1.3. Обезличивание ПДн должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых данных:

– полнота – сохранение всей информации о конкретных субъектах 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 – сохранение семантики ПДн при их обезличивании;

– применимость – возможность решения задач обработки ПДн, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных

целевых программ, без предварительного деобезличивания всего объема записей о субъектах;

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

1.4. Методы обезличивания:

– 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 ПДн путем замены результатами статистической обработки, преобразования, обобщения или удаления части сведений;

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

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

1.5. Требования к свойствам методов обезличивания:

– обратимость (возможность проведения деобезличивания);

– возможность обеспечения заданного уровня анонимности;

– увеличение стойкости при увеличении объема обезличиваемых ПДн.

1.6. Требования к свойствам получаемых обезличенных данных:

– сохранение полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых ПДн);

– сохранение структурированности обезличиваемых ПДн;

– сохранение семантической целостности обезличиваемых ПДн;

– анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений обезличенных данных между собой для деобезличивания).

1.7. Выполнение требований, изложенных в пунктах 1.5 и 1.6 являются критериями выбора для обезличенных данных и применяемых методов обезличивания.

2. Описание методов обезличивания

2.1. Метод введения идентификаторов

Метод реализуется путем замены части ПДн, 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 ПДн, 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 ПДн, 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 – можно 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 ПДн, которые были заменены идентификаторами.

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

Метод введения идентификаторов целесообразно применять при небольшом количестве атрибутов ПДн и небольшом объеме массива ПДн, 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.

2.2. Метод изменения состава или семантики

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

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

– структурированность – связь между отдельными значениями атрибутов ПДн 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 ПДн, 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 ПДн, сохраняющих семантику данных. Изменения должны учитывать специфику задач обработки.

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 можно осуществлять обработку, не требующую деобезличивания всего объема данных о субъектах.

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

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

Метод изменения состава и семантики целесообразно применять в случае, когда возможно изменение состава и семантики, так, что задачи обработки ПДн 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.

2.3. Метод декомпозиции

Метод реализуется путем разделения множества атрибутов ПДн 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 ПДн 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 можно 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 ПДн.

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

2.4. Метод перемешивания

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

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

– полнота – вся информация о субъектах ПДн 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 можно 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 ПДн.

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

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

3. Организация обработки обезличенных данных

3.1. При использовании процедуры обезличивания не допускается совместное хранение ПДн и обезличенных данных.

3.2. Обезличивание ПДн субъектов должно производиться перед внесением их в информационную систему.

3.3. 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 ПДн.

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

3.5. Обработка ПДн при отсутствии квалифицированного персонала либо достаточных материально-технических средств возможна с привлечением сторонних организаций (далее – Операторов) на основании договора.

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

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

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

3.9. Следует вести архив запросов на обработку данных.

3.10. Субъект ПДн должен иметь возможность получить сведения о составе его ПДн, имеющихся у Оператора.

3.11. 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.

3.12. Процедуры обезличивания/деобезличивания должны встраиваться в процессы обработки ПДн как их неотъемлемый элемент, а также максимально эффективно использовать имеющуюся у Оператора инфраструктуру, обеспечивающую обработку ПДн. 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. Порядок работы с обезличенными данными

4.1. Ответственному за организацию обработки ПДн, а также назначенному лицу, выполняющему обезличивание или деобезличивание ПДн, следует:

– обеспечить соответствие процедур обезличивания или деобезличивания ПДн требованиям к обезличенным данным и методам обезличивания;

– обеспечить соответствие процедур обезличивания или деобезличивания условиям и целям обработки ПДн;

– убедиться, что при реализации процедур обезличивания или деобезличивания, а также при последующей обработке обезличенных данных не нарушаются права субъекта ПДн.

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

4.2. В процессе реализации процедуры обезличивания ПДн следует соблюдать все регламентные требования, предъявляемые к выбранному способу реализации процедуры обезличивания.

4.3. При хранении обезличенных данных 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.

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

4.5. В ходе реализации процедуры деобезличивания следует:

– реализовать все требования по обеспечению безопасности получаемых ПДн 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 законодательства Российской Федерации в области ПДн.

5. Выбор методов и процедур обезличивания ПДн

5.1. При выборе методов и процедур обезличивания ПДн следует руководствоваться целями и задачами обработки ПДн. Обезличивание ПДн, обработка которых осуществляется с разными целями, может осуществляться разными методами. Возможно объединение различных методов обезличивания в одну процедуру.

5.2. Для решения каждой задачи обработки определяются требуемые свойства обезличенных данных и метода обезличивания, которые зависят от набора действий, осуществляемых с ПДн (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.

5.3. При выборе метода и процедуры обезличивания также следует учитывать:

– объем ПДн, подлежащих обезличиванию (некоторые методы неэффективны на малых объемах);

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

– область обработки обезличенных данных;

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

– применяемые в информационной системе меры по обеспечению безопасности данных.

5.4. Рекомендации по выбору методов обезличивания в соответствии с классом задач обработки представлены в Приложении 1 к настоящим Правилам. Рекомендации содержат типовые классы задач, состоящие из наиболее часто встречающихся задач обработки ПДн. Проведенная классификация позволяет применять наиболее эффективные для данного класса методы. Рекомендованные методы ранжированы в порядке убывания эффективности их применения.

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

5.6. На каждый класс задач (процесс, случай и т.д.) обезличивания ПДн в Университете следует выпускать отдельный приказ Университета с указанием ответственных лиц, объемов, методов и целей обезличивания ПДн.

Приложение 1
к Правилам обезличивания
персональных данных и работы с ними
в ГБОУВО РК КИПУ имени Февзи
Якубова

Методы обезличивания персональных данных

Класс задач	Задачи обработки	Метод обезличивания
Статистическая обработка и статистические исследования ПДн	Осуществление выборки по заявленным параметрам; проведение исследований по заданным параметрам субъектов.	Метод перемешивания; метод декомпозиции; метод изменения состава или семантики.
Сбор и хранение ПДн	Внесение ПДн субъектов в информационную систему на основе анкет, заявлений и прочих документов.	Метод декомпозиции; 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 ПДн; выдача справок, выписок, уведомлений по запросам субъектов или уполномоченных органов.	Метод перемешивания; метод декомпозиции; метод введения идентификаторов.
Актуализация ПДн	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 ПДн	Поиск информации о субъектах; передача данных смежным органам.	Метод перемешивания; метод декомпозиции; метод введения идентификаторов.
Ведение учета субъектов ПДн	Прием анкет, заявлений; ведение учета ПДн в соответствии с функциями органа.	Метод декомпозиции; метод перемешивания; метод введения идентификаторов.