

Правила работы с обезличенными персональными данными в МАОУ СОШ № 2

1. Общие положения

1.1. Настоящие Правила работы с обезличенными персональными данными разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и методических рекомендаций по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

1.2. Настоящие Правила определяют порядок работы с обезличенными персональными данными.

1.3. Настоящие Правила используются в работе Администратором безопасности и пользователями, осуществляющими обезличивание персональных данных.

1.4. Настоящие Правила утверждаются приказом руководителя МАОУ СОШ № 2 (далее – Учреждение).

2. Термины и определения

Для целей настоящих Правил используются следующие термины:

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.2. 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 персональных данных.

2.3. Оператор – государственный орган или муниципальный орган, организация, 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.

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

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

2.6. 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.

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

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

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

3. Методология выбора методов и процедур обезличивания

3.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, минимизации рисков причинения вреда конкретным гражданам в случае утечки их персональных данных из информационных систем или в случае утраты необходимости в достижении целей обработки, если иное не предусмотрено федеральным законом.

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

3.3. Обезличивание персональных данных, обработка которых осуществляется с разными целями, может осуществляться разными методами, в зависимости от требуемых свойств.

3.3.1. Свойства обезличенных данных:

- полнота - сохранение всей информации о персональных данных конкретных субъектов или группах субъектов, которая имелаась 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.

3.3.2. Наличие перечисленных свойств обеспечивается применяемыми методами обезличивания, к которым 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.

3.4. Для решения каждой задачи обработки необходимо определять требуемые свойства обезличенных данных и метод обезличивания, которые зависят от набора действий, осуществляемых 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).

3.5. Возможно объединение различных методов обезличивания в одну процедуру.

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

3.5.2. Различные способы реализации одной процедуры должны обеспечивать одинаковые результаты.

3.5.3. 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.

3.6. Руководитель Учреждения принимает решение о необходимости обезличивания персональных данных.

3.7. При выборе метода и процедуры обезличивания так же следует учитывать:

- объем персональных данных, подлежащих обезличиванию (некоторые методы неэффективны для малых объемов);
- 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 меры по обеспечению безопасности данных.

4. Порядок работы с обезличенными персональными данными

4.1. Не допускается совместное хранение персональных данных и обезличенных данных.

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

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

4.4. 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.

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

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

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

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

4.9. 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.

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

4.11. В ходе реализации процедуры деобезличивания 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».