



# Администрация муниципального образования город Салехард

## РАСПОРЯЖЕНИЕ

06 декабря 2016 года

№ 2048-р

### **О реализации некоторых мероприятий в сфере обработки персональных данных в Администрации города Салехарда**

В соответствии с частью 3 статьи 18.1 Федерального закона от 27 июля 2006 № 152-ФЗ «О персональных данных» и в целях реализации постановления Правительства Российской Федерации от 21 марта 2012 № 211 «Об утверждении перечня 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»:

1. Утвердить:

1.1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации города Салехарда (Приложение № 1);

1.2. Правила работы с обезличенными данными, обрабатываемыми в Администрации города Салехарда (Приложение № 2);

1.3. Типовую форму обязательства о неразглашении информации, содержащей персональные данные (Приложение № 3);

1.4. Типовую форму согласия на обработку персональных данных сотрудника (Приложение № 4);

1.5. Типовую форму согласия на обработку персональных данных иных субъектов персональных данных (Приложение № 5);

1.6. Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (Приложение № 6);

1.7. Типовую форму обязательства сотрудника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора (контракта) и

прекращении обработки персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (Приложение № 7).

2. Руководителям структурных подразделений Администрации города Салехарда, обладающим правами юридических лиц, принять аналогичные документы, указанных в пункте 1 настоящего распоряжения и обеспечить выполнение обязанностей оператора согласно действующего законодательства Российской Федерации.

3. Признать утратившими силу следующие распоряжения Администрации города Салехарда:

- от 27 августа 2008 года № 789-р «О допуске к персональным данным работников и организации передачи информации о работниках Администрации города Салехарда»;

- от 24 июля 2009 года № 714-р «Об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- от 09 февраля 2009 года № 89-р «О внесении изменений в распоряжение Администрации города Салехарда от 27 августа 2008 года № 789-р».

Глава Администрации города

И.Л. Кононенко

**ПРАВИЛА**  
**осуществления внутреннего контроля соответствия обработки**  
**персональных данных требованиям к защите персональных данных**  
**в Администрации города Салехарда**

**1. Общие положения**

1.1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации города Салехарда (далее - Правила) устанавливаются процедуры (основания, порядок и формы) проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами» и другими нормативными правовыми актами.

1.3. Целью настоящих Правил является выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных.

1.4. В Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

**2. Процедуры, направленные на выявление и предотвращение**  
**нарушений законодательства Российской Федерации**  
**в сфере персональных данных**

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Администрации города Салехарда (далее – Администрация города) организовывается проведение проверок условий обработки персональных данных.

2.2. Проверки условий обработки персональных данных на соответствие требованиям к защите персональных данных, установленных в Администрации города осуществляются комиссией, создаваемой распоряжением Администрации города. В состав комиссии входит председатель комиссии (один из заместителей Главы Администрации города) и не менее трех членов комиссии (сотрудников Администрации города). Проверки могут быть плановыми и внеплановыми (далее - Проверки).

2.3. Плановые проверки проводятся в соответствии с ежегодным планом проведения проверок, разрабатываемым структурным подразделением, выполняющим функции по технической защите (безопасности) информации, и утверждается распоряжением Администрации города. Периодичность плановой проверки не реже одного раза в квартал. Срок проведения плановой проверки составляет не более трех рабочих дней.

2.4. Внеплановые проверки проводятся на основании поступившего в Администрацию города письменного заявления субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных о нарушениях правил обработки персональных данных.

2.5. В течение трех рабочих дней с момента поступления в Администрацию города заявления о нарушениях правил обработки персональных данных принимается решение о проведении внеплановой проверки, которое оформляется распоряжением Администрации города.

2.6. Проведение внеплановой проверки организуется в течение трех рабочих дней с момента издания распоряжения Администрации города о проведении внеплановой проверки и должна быть завершена не позднее чем через месяц со дня ее назначения.

2.7. При проведении Проверок условий обработки персональных данных должен быть полностью, объективно и всесторонне исследован порядок обработки персональных данных и его соответствие требованиям обработки персональных данных, установленным в Администрации города, а именно:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление мероприятий по обеспечению целостности персональных данных.

2.8. В случае выявления фактов нарушений требований обработки персональных данных, а именно:

- несоблюдения установленного порядка обработки персональных данных;

- несоблюдения условий хранения носителей персональных данных;

- использования средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;

- нарушения заданного уровня безопасности персональных данных (конфиденциальность/целостность/доступность), в обязательном порядке устанавливаются причины нарушения обработки персональных данных и наличие (отсутствие) вины.

Комиссия имеет право:

- запрашивать у сотрудников Администрации города информацию, необходимую для реализации своих полномочий;

- требовать от уполномоченных на обработку персональных данных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить Главе Администрации города или заместителю Главы Администрации города предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить Главе Администрации города или заместителю Главы Администрации города

предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.10. По результатам Проверок комиссии, администратором информационной безопасности составляется план устранения выявленных нарушений, который доводится до руководителя проверенного подразделения.

2.11. В случаях выявления нарушений обработки персональных данных, требующих немедленного устранения, принимаются меры оперативного реагирования.

2.12. Результаты внутреннего контроля оформляются в виде справки. Справка о результатах проведенных Проверок, перечень мероприятий по устранению выявленных нарушений и сроки их устранения направляются для согласования Главе Администрации города за подписью председателя комиссии.

2.13. Устранение выявленных в ходе Проверок нарушений проводится в порядке и сроки, установленные действующим законодательством в сфере обработки персональных данных.

2.14. В отношении персональных данных, ставших известными комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

**ПРАВИЛА**  
**работы с обезличенными данными, обрабатываемыми**  
**в Администрации города Салехарда**

**1. Общие положения**

1.1. Правила работы с обезличенными данными, обрабатываемых в Администрации города Салехарда (далее - Правила) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон), Приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» и постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня 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».

1.2. Настоящие Правила определяют порядок работы с обезличенными персональными данными, обрабатываемыми в Администрации города Салехарда (далее - Администрация города).

**2. Условия и методы обезличивания персональных данных**

2.1. Обезличивание персональных данных может быть проведено с целью снижения ущерба от разглашения защищаемых персональных данных, снижения класса (уровня защищенности) информационных систем персональных данных (далее - ИСПДн), в статистических или иных исследовательских целях, и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки персональных данных. К наиболее перспективным и удобным для практического применения относятся следующие 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 персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);

- метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим отдельным хранением подмножеств);

- метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

2.1.1. Метод введения идентификаторов реализуется путем замены части персональных данных, позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия.

Метод обеспечивает следующие свойства обезличенных данных:

- полнота;
- структурированность;
- семантическая целостность;

- применимость.

Оценка свойств метода:

обратимость (метод позволяет провести процедуру деобезличивания);

вариативность (метод позволяет перейти от одной таблицы соответствия к другой без проведения процедуры деобезличивания);

изменяемость (метод не позволяет вносить изменения в массив обезличенных данных без предварительного деобезличивания);

стойкость (метод не устойчив к атакам, подразумевающим наличие у лица, осуществляющего несанкционированный доступ, частичного или полного доступа к справочнику идентификаторов, стойкость метода не повышается с увеличением объема обезличиваемых персональных данных);

возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);

совместимость (метод позволяет интегрировать записи, соответствующие отдельным атрибутам);

параметрический объем (объем таблицы (таблиц) соответствия определяется числом записей о субъектах, подлежащих обезличиванию);

возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

Для реализации метода требуется установить атрибуты персональных данных, записи которых подлежат замене идентификаторами, разработать систему идентификации, обеспечить ведение и хранение таблиц соответствия.

2.1.2. Метод изменения состава или семантики реализуется путем обобщения, изменения или удаления части сведений, позволяющих идентифицировать субъекта ПДн (далее – субъекта).

Метод обеспечивает следующие свойства обезличенных данных:

- структурированность;

- релевантность;

- применимость;

- анонимность.

Оценка свойств метода:

обратимость (метод не позволяет провести процедуру деобезличивания в полном объеме и применяется при статистической обработке персональных данных);

вариативность (метод не позволяет изменять параметры метода без проведения предварительного деобезличивания);

изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

стойкость (стойкость метода к атакам на идентификацию определяется набором правил реализации, стойкость метода не повышается с увеличением объема обезличиваемых персональных данных);

возможность косвенного деобезличивания (метод исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);

совместимость (метод не обеспечивает интеграции с данными, обезличенными другими методами);

параметрический объем (параметры метода определяются набором правил изменения состава или семантики персональных данных);

возможность оценки качества данных (метод не позволяет проводить анализ, использующий конкретные значения персональных данных).

Для реализации метода требуется выделить атрибуты персональных данных, записи которых подвергаются изменению, определить набор правил внесения изменений и иметь возможность независимого внесения изменений для данных каждого субъекта.

При этом возможно использование статистической обработки отдельных записей данных и замена конкретных значений записей результатами статистической обработки (средние значения, например).

2.1.3. Метод декомпозиции реализуется путем разбиения множества записей персональных данных на несколько подмножеств и создание таблиц, устанавливающих связи между подмножествами, с последующим раздельным хранением записей, соответствующих этим подмножествам.

Метод обеспечивает следующие свойства обезличенных данных:

- полнота;
- структурированность;
- релевантность;
- семантическая целостность;
- применимость.

Оценка свойств метода:

обратимость (метод позволяет провести процедуру деобезличивания);

вариативность (метод позволяет изменить параметры декомпозиции без предварительного деобезличивания);

изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

стойкость (метод не устойчив к атакам, подразумевающим наличие у злоумышленника информации о множестве субъектов или доступа к нескольким частям раздельно хранимых сведений);

возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющих у других операторов);

совместимость (метод обеспечивает интеграцию с данными, обезличенными другими методами);

параметрический объем (определяется числом подмножеств и числом субъектов, массив которых обезличивается, а также правилами разделения персональных данных на части и объемом таблиц

связывания записей, находящихся в различных хранилищах);

возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

Для реализации метода требуется предварительно разработать правила декомпозиции, правила установления соответствия между записями в различных хранилищах, правила внесения изменений и дополнений в записи и хранилища.

2.1.4. Метод перемешивания реализуется путем перемешивания отдельных записей, а также групп записей между собой.

Метод обеспечивает следующие свойства обезличенных данных:

- полнота;
- структурированность;
- релевантность;
- семантическая целостность;
- применимость;
- анонимность.

Оценка свойств метода:

обратимость (метод позволяет провести процедуру деобезличивания);

вариативность (метод позволяет изменять параметры перемешивания без проведения процедуры деобезличивания);

изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

стойкость (длина перестановки и их совокупности определяет стойкость метода к атакам на идентификацию);



возможность косвенного деобезличивания (метод исключает возможность проведения деобезличивания с использованием персональных данных, имеющихся у других операторов);  
совместимость (метод позволяет проводить интеграцию с данными, обезличенными другими методами);

параметрический объем (зависит от заданных методов и правил перемешивания и требуемой стойкости к атакам на идентификацию);

возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

Для реализации метода требуется разработать правила перемешивания и их алгоритмы, правила и алгоритмы деобезличивания и внесения изменений в записи.

Метод может использоваться совместно с методами введения идентификаторов и декомпозиции.

### **3. Порядок работы с обезличенными персональными данными**

3.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности без согласия субъекта, за исключением их обработки для статистической или иной исследовательской деятельности, иных действий, не противоречащих действующему законодательству.

3.2. Обезличенные персональные данные могут обрабатываться с использованием средств автоматизации и без использования таковых.

3.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы с отчуждаемыми носителями (в случае их применения);
- правил резервного копирования;
- инструкции о порядке доступа в помещения, в которых ведется обработка персональных данных.

3.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к бумажным носителям и в помещения, где они хранятся.

Форма

**ОБЯЗАТЕЛЬСТВО**  
**о неразглашении информации, содержащей персональные данные**

Я, \_\_\_\_\_,  
(Ф.И.О.)

исполняющий (ая) должностные обязанности по замещаемой должности

\_\_\_\_\_  
(должность, наименование структурного подразделения)

предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. В течение года после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

\_\_\_\_\_  
(фамилия, инициалы)

\_\_\_\_\_  
(подпись)

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Форма

**СОГЛАСИЕ**  
**на обработку персональных данных сотрудника**

Представителю нанимателя (работодателю)

\_\_\_\_\_ (наименование, адрес, Ф.И.О. руководителя)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

ОТ \_\_\_\_\_

фамилия, инициалы заявителя

\_\_\_\_\_ должность сотрудника

\_\_\_\_\_ наименование структурного подразделения

\_\_\_\_\_ адрес

\_\_\_\_\_ паспорт

Не возражаю против \_\_\_\_\_ Вами сведений обо мне, содержащих  
\_\_\_\_\_ получения/сообщения

данные о: \_\_\_\_\_

\_\_\_\_\_ перечень персональных данных

\_\_\_\_\_ указать, откуда могут быть получены или куда переданы персональные данные

с целью \_\_\_\_\_

\_\_\_\_\_ указать цель обработки персональных данных, в т.ч. для размещения на официальном сайте

Администрации МО город Салехард

в \_\_\_\_\_

\_\_\_\_\_ форме

\_\_\_\_\_ документальной/электронной/устной (по

\_\_\_\_\_ телефону)

в течение \_\_\_\_\_

\_\_\_\_\_ указать срок действия согласия

Настоящее заявление может быть отозвано мной в письменной форме.

Юридические последствия отказа предоставить свои персональные данные мне  
разъяснены.

\_\_\_\_\_ подпись заявителя, дата

Форма

**СОГЛАСИЕ**  
**на обработку персональных данных иных субъектов**  
**персональных данных**

Я, \_\_\_\_\_,  
(фамилия, имя, отчество)  
проживающий (ая) по адресу \_\_\_\_\_,  
зарегистрированный (ая) по адресу \_\_\_\_\_,  
документ, удостоверяющий личность: \_\_\_\_\_  
(наименование, серия (при наличии) и номер документа)

\_\_\_\_\_  
(сведения о дате выдачи документа и выдавшем его органе)  
в соответствии с частью 1 статьи 9 Федерального закона от 27 июля 2006 года  
№ 152-ФЗ «О персональных данных» в целях предоставления мне муниципальных  
услуг/исполнения муниципальных функций по

\_\_\_\_\_  
(указывается наименование услуги, функции)  
даю согласие оператору персональных данных на осуществление действий (операций) с  
моими персональными данными, включая сбор, запись, систематизацию, накопление,  
хранение, уточнение (обновление, изменение), извлечение, использование, передачу  
(распространение, предоставление, доступ), обезличивание, блокирование, удаление в  
документальной, электронной, устной форме.

\_\_\_\_\_  
(дата)

\_\_\_\_\_  
(подпись)

Форма

**РАЗЪЯСНЕНИЯ**  
**субъекту персональных данных юридических последствий отказа предоставить свои**  
**персональные данные**

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» уведомляем Вас, что обязанность предоставления Вами персональных данных установлена

---

(реквизиты и наименование нормативных правовых актов)

В случае отказа Вами предоставить свои персональные данные оператор не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям:

---

(перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи, иным образом затрагивающие его права, свободы и законные интересы)

В соответствии с законодательством в области персональных данных Вы имеете право:

на получение сведений об операторе, о месте его нахождения, о наличии у оператора своих персональных данных, а также на ознакомление с такими персональными данными;

требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

на получение при обращении или при направлении запроса информации, касающейся обработки своих персональных данных;

на обжалование действия или бездействия оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

---

(дата)

---

(подпись)

---

(расшифровка)

Форма

### ОБЯЗАТЕЛЬСТВО

**сотрудника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора (контракта) и прекращении обработки персональных данных, ставших известными ему в связи с исполнением должностных обязанностей**

Я, \_\_\_\_\_ (Ф.И.О.),  
исполняющий(ая) \_\_\_\_\_ должностные обязанности по замещаемой должности \_\_\_\_\_

\_\_\_\_\_ (должность, наименование структурного подразделения), предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к конфиденциальной информации (персональным данным), не содержащей сведений, составляющих государственную тайну. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доведены (будут доведены) или станут известными в связи с выполнением должностных обязанностей.

2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доведены (будут доведены) или станут известными в связи с выполнением должностных обязанностей.

3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному начальнику, а также лицу, ответственному за организацию защиты информации в \_\_\_\_\_ (наименование структурного подразделения Администрации муниципального образования город Салехард).

4. Не использовать конфиденциальные сведения с целью получения выгоды.

5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.

6. После прекращения трудового договора и увольнения с муниципальной службы (работы) не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

\_\_\_\_\_  
Ф.И.О.

\_\_\_\_\_  
подпись

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.