Методические рекомендации
по организации обработки и обеспечению безопасности персональных данных

Содержание

Перечень сокращений

В настоящем документе используются сокращения, приведенные в таблице 1.

Таблица 1 − Перечень сокращений

Сокращение	Обозначение
ИСПДн	Информационная система персональных данных
Организация	Орган исполнительной власти города Москвы, государственное учреждение города Москвы и иные организации, подведомственные органам исполнительной власти города Москвы
ПДн	Персональные данные
ФЗ	Федеральный закон
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

Перечень терминов

В настоящем документе используются термины, приведенные в таблице 2.

Таблица 2 − Перечень терминов

Термин	Определение	Источник
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники	Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»
Аттестация объектов информатизации	Комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации	ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний
Безопасность информации	Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность	ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
Доступ к информации	Возможность получения информации и ее использования	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Термин	Определение	Источник
Защита информации	Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию	ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств	Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»
Модель угроз безопасности информации (персональных данных)	Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.	ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
Обезличивание персональных данных	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных	Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»
Обладатель информации	Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите 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 персональных данных	Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»
Оператор	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами	Федеральный закон Российской Федерации от 27.07.2006 г. № 152-

Термин	Определение	Источник
	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	ФЗ «О персональных данных»
Оператор информационной системы	Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Оценка соответствия требованиям по защите информации	Прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты, информации	ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»
Система защиты информации	Совокупность органов и (или) исполните-лей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленными соответствующими документами в области защиты информации	ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
Средство защиты информации	Техническое, программное, программно-техническое средство, вещество и/или материал, предназначенное или используемое для защиты информации	ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
Требование по защите информации	Установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации	ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
Угроза безопасности информации (персональных данных)	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации	ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

1 Общие положения

Настоящие Методические рекомендации по организации обработки и обеспечению безопасности персональных данных (далее – Методические рекомендации) содержат методику проведения работ по приведению деятельности органов исполнительной власти города Москвы, государственных учреждений города Москвы и иных организаций, подведомственных органам исполнительной власти города Москвы (далее – Организации) в области обработки и обеспечения безопасности персональных данных в соответствие требованиям законодательства Российской Федерации.

Методические рекомендации в основном затрагивают вопросы, связанные с подготовкой организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных, и упорядочиванием процессов обработки персональных данных в Организациях как при обработке персональных данных в информационных системах персональных данных (далее – ИСПДн), так и при обработке персональных данных (далее – ПДн), осуществляемой без использования средств автоматизации. Методические рекомендации содержат примерные формы организационно-распорядительных документов, разработанные с учетом требований законодательства Российской Федерации в области обработки и обеспечения безопасности ПДн, а также рекомендации по их адаптации к конкретным условиям обработки ПДн в Организации. Организация самостоятельно определяет потребность в разработке, актуализации организационно-распорядительных документов и их содержание.

Организация несет ответственность в соответствии с нормами действующего законодательства Российской Федерации за форму и содержание организационно-распорядительных документов, разработанных на основании Методических рекомендаций, в том числе примерных форм документов.

2 Нормативные ссылки

Процессы обработки и обеспечения безопасности ПДн в Организациях регламентируются следующими нормативными правовыми актами Российской Федерации:

- Конституция Российской Федерации от 12 декабря 1993 г.;
- Трудовой кодекс Российской Федерации от 20 декабря 2001 г. № 197-ФЗ;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

– Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»;

– Распоряжение Правительства Москвы от 03 июля 2012 г. № 342-РП «О требованиях к вводу в эксплуатацию информационных систем, создаваемых в городе Москве»;

– Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказ Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»;

– Приказ Роскомнадзора от 15.03.2013 № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных»;

– Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

3 Структура мероприятий по выполнению норм законодательства в области обработки и защиты персональных данных

В общем случае, мероприятия по выполнению норм законодательства в области обработки и защиты ПДн можно поделить на три основных блока:

1) меры, определяющие порядок обработки ПДн (организационные и правовые меры, определяющие порядок обработки ПДн в Организации в целом);

2) меры по обеспечению безопасности ПДн при их обработке в информационных системах (организационные и технические меры, направленные на обеспечение безопасности ПДн при их обработке в информационных системах);

3) контроль соответствия обработки ПДн требованиям законодательства в области обработки и защиты ПДн.

Далее в Методических рекомендациях будет рассмотрены блоки мер 1 и 3.

В связи с тем, что в подавляющем большинстве случаев информационные системы, в которых обрабатываются ПДн, являются государственными информационными системами, основные правила реализации мероприятий блока 2 определяются требованиями, предъявляемыми к государственными информационным системам и рассматриваются в «Методических рекомендациях по обеспечению защиты информации в государственных информационных системах». В Методических рекомендациях приведена только специфика реализации мероприятий блока 2, связанная с наличием и обработкой ПДн в информационных системах.

4 Основные организационные и правовые меры, определяющие порядок обработки персональных данных в Организации

4.1 Подготовительные мероприятия. Сбор исходных данных и описание процессов обработки персональных данных

Для определения и реализации мер, необходимых для приведения деятельности Организации в области обработки ПДн в соответствие требованиям законодательства, необходимо провести инвентаризацию процессов обработки ПДн в Организации.

Для определения процессов обработки ПДн необходимо проанализировать нормативные правовые акты и организационно-распорядительные документы, регламентирующие деятельность Организации, в рамках которой осуществляется (может осуществляться) обработка ПДн. Также могут использоваться опросные листы, рассылаемые по структурным подразделениям Организации.

На основании первичного анализа опросных листов выявляется примерный перечень структурных подразделений, в которых может осуществляться обработка ПДн, и перечень информационных систем, в которых может осуществляться обработка ПДн.

После того, как все собранные данные проанализированы и обобщены, можно получить примерный перечень процессов, в рамках функционирования которых осуществляется обработка ПДн.

Наиболее распространенными процессами обработки ПДн в Организации являются:

– кадровый учет;

– подбор персонала;

– бухгалтерская отчетность, расчет заработной платы, расчет налогов и социальных выплат;

– воинский учет;

– рассмотрение заявок участников закупок;

– обработка обращений граждан, юридических лиц, органов государственной власти;

– оказание государственных или муниципальных услуг;

– договорная работа с контрагентами;

– претензионная и судебная работа юридической службы и др.

В зависимости от специфики деятельности Организации и ее организационно-правовой формы перечень процессов обработки ПДн будет корректироваться.

Далее **по каждому процессу обработки ПДн** необходимо определить:

– цели обработки ПДн;

– категории субъектов ПДн, данные которых обрабатываются в рамках процесса (с привязкой к цели обработки);

– применимое законодательство (с привязкой к цели обработки) – правовое основание обработки ПДн;

– сроки обработки (в т.ч. хранения) ПДн;

– перечень ПДн (с привязкой к цели обработки и к категории субъекта ПДн);

– способы обработки ПДн (с использованием средств автоматизации, без использования средств автоматизации, смешанный);

– перечень информационных систем, в которых обрабатываются ПДн;

– перечень мест хранения материальных носителей ПДн;

– перечень лиц, осуществляющих обработку ПДн;

– порядок обработки ПДн в рамках процесса.

Указанные данные могут быть получены путем проведения интервью с владельцами процессов. По результатам анализа собранных данных возможно уточнение перечня процессов обработки ПДн.

Отметим, что наиболее распространенными категориями субъектов ПДн, ПДн которых обрабатываются в Организации, могут быть:

– работники Организации (либо государственные гражданские служащие);

– ближайшие родственники работников (государственных гражданских служащих);

– уволенные работники (государственные гражданские служащие);

– кандидаты на замещение вакантных должностей;

– представители организаций – участников закупок, проводимых Организацией;

– представители контрагентов;

– физические лица, обратившиеся в Организацию с жалобой, предложением, заявлением или направившие запрос о предоставлении информации о деятельности Организации;

– физические лица, предоставившие свои персональные данные в рамках исполнения Организацией своих полномочий и т.д.

В зависимости от специфики деятельности Организации и ее организационно-правовой формы перечень категорий субъектов ПДн будет корректироваться.

Для выявленных информационных систем Организации, в которых обрабатываются ПДн (ИСПДн), необходимо определить назначение (цель обработки ПДн в этой ИСПДн), категории и объем обрабатываемых ПДн в соответствии с постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119.

Необходимо иметь в виду, что возможны случаи, когда Организация будет являться оператором ИСПДн, но не будет являться оператором ПДн, обрабатываемых в этих ИСПДн.

Соответственно, необходимо различать случаи, когда Организация является оператором ПДн (примером, применимым для каждой Организации является обработка ПДн работников этой Организации) и случаи, когда Организация является оператором информационной системы, в которой обрабатываются ПДн.

В последнем случае цели обработки ПДн, правовые основания обработки, категории субъектов ПДн и состав обрабатываемых ПДн определяются не Организацией, а оператором этих ПДн (обладателем информации).

Отметим, что если в правовом акте Правительства Москвы определяется орган исполнительной власти города Москвы, ответственный за организацию информационного наполнения информационной системы, полномочия по организации обработки персональных данных, содержащихся в информационной системе, определению целей обработки таких персональных данных, а также полномочия обладателя информации, содержащейся в информационной системе, возлагаются на указанный орган исполнительной власти города Москвы.

В результате должен быть составлен перечень информационных систем Организации, в которых обрабатываются ПДн.

4.2 Ответственность за организацию обработки персональных данных

Назначение лица, ответственного за организацию обработки ПДн (далее – Ответственный за организацию обработки ПДн) предусмотрено пунктом 1 части 1 статьи 18.1 и статьей 22.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»).

При назначении Ответственного за организацию обработки ПДн необходимо иметь в виду, что в соответствии с частью 2 статьи 22.1 Ответственный за организацию обработки ПДн должен получать указания непосредственно от исполнительного органа Организации и быть подотчетным ему.

В Организации может быть назначен только один Ответственный за организацию обработки ПДн. При этом часть своих функций Ответственный за организацию обработки ПДн может делегировать другим работникам Организации (например, владельцам процессов обработки ПДн), которые будут отвечать перед ним за организацию обработки ПДн в рамках свое направления (переданных функций), однако ответственность за организацию обработки ПДн в рамках Организации в целом будет нести Ответственный за организацию обработки ПДн.

В соответствии с частью 4 статьи 22.1 ФЗ «О персональных данных» Ответственный за организацию обработки ПДн, в частности, обязан:

– осуществлять внутренний контроль соблюдения оператором и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

– доводить до сведения работников оператора положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

– организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль приема и обработки таких обращений и запросов.

Следует отметить, что приведенный перечень обязанностей не является исчерпывающим. Организация вправе возложить на Ответственного за организацию обработки ПДн дополнительные обязанности, выполнение которых позволит обеспечить защиту прав субъектов ПДн, ПДн которых обрабатываются организацией.

Полномочия Ответственного за организацию обработки ПДн устанавливаются Организацией исходя из возложенных на это лицо обязанностей.

С целью назначения Ответственного за организацию обработки ПДн Организация может **приказом о внесении изменений в штатное расписание** ввести новую должность Ответственного за организацию обработки ПДн, либо приказом (распоряжением) **назначить должностное лицо (работника) Организации ответственным за организацию обработки ПДн**, внеся соответствующие изменения в его должностную инструкцию.

К функциям Ответственного за организацию обработки ПДн могут быть отнесены:

– контроль проведения мероприятий по защите персональных данных;

– обеспечение ведения учета процессов обработки ПДн в Организации и поддержания документации по указанным процессам в актуальном виде;

– организация и осуществление внутреннего контроля соблюдения Организацией и ее работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн

– организация и контроль проведения обучения работников Организации в области обработки и защиты персональных данных;

– организация и контроль проведения проверки знаний работников Организации в области обработки и защиты персональных данных;

– организация приема и обработки обращений и запросов субъектов ПДн и запросов уполномоченного органа по защите прав субъектов ПДн;

– организация и контроль разработки и своевременной актуализации внутренних организационно-распорядительных документов Организации в области обработки и защиты ПДн;

– контроль проведения мероприятий по результатам разрешения и расследования инцидентов информационной безопасности, связанных с нарушением требований по обработке и защите персональных данных;

– контроль включения Организации в план проверок регулирующих органов;

– информирование руководства Организации о предстоящей проверке регулирующими органами;

– координацию подготовки Организации к прохождению проверки регулирующими органами;

– сопровождение (организацию сопровождения) должностного лица уполномоченного органа в ходе проверки (предоставление (организация предоставления) необходимых документов и информации и т.д.).

Необходимо отметить, что в функции Ответственного за организацию обработки ПДн не входит обеспечение безопасности ПДн.

4.3 Согласие субъекта персональных данных на обработку персональных данных

Одним из краеугольных моментов корректности обработки ПДн в Организации является наличие правового основания обработки ПДн.

Для **каждого выявленного процесса обработки ПДн** необходимо провести анализ необходимости предоставления субъектом ПДн согласия на обработку ПДн.

В соответствии с ФЗ «О персональных данных» обработка ПДн может осуществляться без согласия субъекта ПДн в следующих случаях:

– обработка ПДн необходима для осуществления Организацией функций, возложенных законодательством Российской Федерации;

– обработка ПДн необходима для исполнения судебного акта;

– обработка ПДн необходима для исполнения полномочий исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных

Федеральным законом от 27 июля 2010 г. №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта ПДн на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

– обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

– обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

– обработка ПДн необходима для осуществления прав и законных интересов Организации или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

– осуществляется обработка ПДн, сделанных общедоступными субъектом персональных данных;

– осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Далее также по каждому процессу обработки ПДн необходимо определить вид согласия на обработку ПДн в случае, если оно необходимо – письменная или иная форма.

Обработка ПДн может осуществляться при наличии согласия субъекта ПДн в письменной форме (за исключением случаев, предусмотренных законодательством) в следующих случаях:

– при включении ПДн в общедоступные источники ПДн;

– при обработке специальных категорий ПДн;

– при обработке биометрических ПДн для установления личности субъекта ПДн;

– при трансграничной передаче ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн;

– при принятии решений, порождающих юридические последствия, на основании исключительно автоматизированной обработки ПДн;

– при передаче/получении ПДн работников Организации третьим лицам/от третьих лиц, осуществляемой не в рамках исполнения трудового законодательства.

Требования к форме письменного согласия субъекта ПДн на обработку его ПДн установлены п.4 ст.9 ФЗ «О персональных данных» и определяют необходимость наличия следующих сведений:

– фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи

указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);

– наименование или фамилию, имя, отчество и адрес Организации;

– цель обработки ПДн;

– перечень ПДн, на обработку которых дается согласие;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Организации, если обработка будет поручена такому лицу;

– перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых Организацией способов обработки ПДн;

– срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва;

– подпись субъекта ПДн.

Необходимо обратить внимание, что в согласии на обработку ПДн в письменной форме должна быть указана только одна цель обработки ПДн.

В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн должны проверяться Организацией.

Отметим, что получение/передача Организацией ПДн работника от третьих лиц/третьим лицам осуществляется с письменного согласия работника в каждом конкретном случае получения/передачи ПДн, за исключением случаев, предусмотренных законодательством Российской Федерации.

Далее необходимо разработать и утвердить формы согласий субъекта ПДн на обработку ПДн и порядок получения согласия субъекта ПДн на обработку ПДн для всех необходимых случаев.

Ниже по тексту приведен пример формы согласия работника Организации на передачу его ПДн сторонней организации в целях их включения в общедоступные источники ПДн.

Руководителю МБОУ ДО Катангский ЦДО

_____,
(фамилия, имя и отчество субъекта персональных данных)

паспорт _____,
(серия и номер паспорта)

_____
(кем и когда выдан паспорт)

Адрес регистрации по месту жительства

_____

Согласие на передачу персональных данных

Настоящим, своей волей и в своем интересе, в соответствии со статьей 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» выражаю(даю) свое согласие МБОУ ДО Катангский ЦДО

(юридический адрес: 666611, Российская Федерация, Иркутская область, Катангский район, с. Ербогачен, ул. Ленина, 5) на передачу МБОУ ДО Катангский ЦДО

(юридический адрес: 666611, Российская Федерация, Иркутская область, Катангский район, с. Ербогачен, ул. Ленина, 5) с использованием средств автоматизации с целью формирования внутренних информационных систем, ресурсов, справочников, баз данных, которые являются общедоступными источниками персональных данных, своих персональных данных:

- фамилия, имя, отчество;
- фотографическое изображение;
- дата рождения;
- рабочие номера телефонов и адрес электронной почты;
- номера мобильных телефонов;
- сведения о должности, подразделении, периоды отпусков (отсутствия).

Настоящее согласие предоставляется на срок действия трудового договора (*для органа исполнительной власти указать: служебного контракта государственного гражданского служащего*) и может быть отозвано в соответствии с частью 2 статьи 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» на основании письменного заявления в произвольной форме.

Условия настоящего Согласия мной лично прочитаны и мне понятны.

_____,
собственноручно указывается СОГЛАСЕН (СОГЛАСНА)

_____,
собственноручно **полностью** указывается фамилия, имя, отчество (если имеется)

_____ Дата:_____ _____20__г.
подпись

4.4 Типовые формы

Используемые в Организации типовые формы должны соответствовать требования Постановления Правительства от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Необходимо провести анализ типовых форм на предмет соответствия требованиям Постановления Правительства от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и внести в них корректировки в случае необходимости. При этом нужно иметь в виду, что изменения могут вноситься только в те типовые формы, которые разрабатывались непосредственно самой Организацией.

4.5 Разработка и ввод в действие организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных

В Организации должны быть разработаны и внедрены внутренние документы по вопросам обработки и обеспечения безопасности ПДн. Основания для разработки организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных приведены в Приложении 1.

Рекомендуется разработать следующие организационно-распорядительные документы по вопросам обработки и обеспечения безопасности ПДн (с учетом их применимости к специфике деятельности конкретной Организации):

- Политика в отношении обработки персональных данных (Приложение 2);
- Правила обработки персональных данных (Приложение 3);
- Правила рассмотрения запросов субъектов персональных данных или их представителей (Приложение 4);
- Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение 5);
- Правила работы с обезличенными данными (Приложение 6);
- Перечень должностей работников, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- Перечень ИСПДн;
- Перечень персональных данных (Приложение 7);
- Перечень должностей работников, замещение которых предусматривает осуществление обработки персональных данных (Приложение 8);
- Перечень мест хранения материальных носителей персональных данных (Приложение 9);
- Должностные обязанности ответственного за организацию обработки персональных данных;
- Обязательство о неразглашении и обеспечении безопасности персональных данных (Приложение 10);
- Типовое обязательство работника о прекращении обработки персональных данных в случае расторжения с ним трудового договора (Приложение 11);
- Типовая форма согласия на обработку персональных данных работника;

– Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (Приложение 12);

– Порядок доступа в помещения, в которых ведется обработка персональных данных.

Приведенные документы должны быть утверждены приказом (распоряжением) по Организации.

В Приложениях 2-12 к Методическим рекомендациям приведены примеры только тех организационно-распорядительных документов, для которых можно выделить типовые требования и правила обработки ПДн. Рекомендации по содержанию остальных организационно-распорядительных документов приведены по тексту Методических рекомендаций.

Политика в отношении обработки персональных данных и сведения о реализуемых требованиях к защите ПДн должны быть опубликованы на сайте Организации, либо к ним должен быть обеспечен неограниченный доступ иным способом.

Правила обработки персональных данных должны быть определены и описаны для каждой категории субъектов ПДн. Документирование правил обработки ПДн возможно осуществлять отдельно для каждого процесса обработки ПДн, отдельно для каждого структурного подразделения, участвующего в процессе обработки ПДн, либо возможно описание в одном документе общей совокупности правил обработки ПДн. При этом рекомендуется правила обработки ПДн работников выделять в отдельный документ.

Правила работы с обезличенными данными разрабатываются только в случае, если Организация осуществляет обезличивание ПДн. **Перечень должностей работников, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных**, также разрабатывается только в случае осуществления Организацией обезличивания ПДн. Также отметим, что перечень указанных должностей может быть либо утвержден отдельным перечнем, либо включен в состав Правил работы с обезличенными данными. В любом случае, при осуществлении Организацией обезличивания ПДн, должны быть назначены ответственные работники, участвующие в процессе обезличивания ПДн.

Должностные обязанности ответственного за организацию обработки персональных данных описаны в разделе 4.2 настоящих Методических рекомендаций.

Требования к содержанию и видам **согласия на обработку ПДн** субъектов ПДн приведены в разделе 4.3 настоящих Методических рекомендаций.

В организационно-распорядительных документах Организации, устанавливающих **правила пропускного режима и охраны помещений**, должны быть определены основные требования к организации пропускного режима и охраны помещений в пределах охраняемой территории, на которой располагаются информационные ресурсы и материальные носители информации, с целью

обеспечения защиты от несанкционированного доступа к персональным данным. В правилах пропускного режима необходимо отразить порядок ведения журналов (реестров, книг) однократного пропуска субъекта ПДн на территорию Организации – в том случае, если такие журналы (реестры, книги) ведутся.

Перечни и типовые формы документов могут быть утверждены в виде отдельных документов либо в составе организационно-распорядительных документов Организации, описывающих процедуры (правила) обработки и обеспечения безопасности ПДн.

Необходимые пояснения к положениям примеров организационно-распорядительных документов выделены курсивом по тексту.

4.6 Ознакомление работников, осуществляющих обработку персональных данных, с правилами обработки и требованиями к защите персональных данных и (или) организация обучения указанных работников

Все работники Организации должны быть ознакомлены не только с внутренними документами Организации, касающимися обработки и обеспечения безопасности ПДн, но и с положениями законодательства Российской Федерации в области обработки и защиты ПДн.

При этом факт ознакомления работников Организации правилами и требованиями должен быть задокументирован.

4.7 Поручение оператора на обработку персональных данных

В соответствии с ч.3 ст.6 ФЗ «О персональных данных» Организация вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, на основании заключаемого с этим лицом договора (государственного или муниципального контракта), либо путем принятия государственным или муниципальным органом соответствующего акта (поручение оператора). Также обработка ПДн может быть поручена Организации третьими лицами.

Необходимо провести анализ выявленных процессов обработки ПДн на предмет необходимости наличия поручения оператора и провести анализ имеющихся поручений оператора на предмет их соответствия требованиям ч.3 ст.6 ФЗ «О персональных данных».

4.8 Уведомление об обработке персональных данных

Организация до начала обработки ПДн обязана уведомить уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор) о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных ч.2 ст.22 ФЗ «О персональных данных». Требования к содержанию уведомления приведены в ч.3 ст.22 ФЗ «О персональных данных». В случае изменения сведений, содержащихся в ранее направленном Организацией уведомлении, а также в случае прекращения обработки

ПДн Организация обязана уведомить об этом Роскомнадзор в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки ПДн.

Уведомление о намерении осуществлять обработку ПДн заполняется на сайте Роскомнадзора по адресу http://rkn.gov.ru/personal-data/forms/notification/, после чего электронное уведомление необходимо отправить в информационную систему Роскомнадзора, подготовить заполненную форму к распечатке, распечатать на бланке Организации, подписать у руководителя Организации и направить заказным письмом в Управление Роскомнадзора по Центральному федеральному округу.

Информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку ПДн, заполняется на сайте Роскомнадзора по адресу http://rkn.gov.ru/personal-data/forms/p333/, при этом заполняются только те поля информационного письма, в которые вносятся изменения. Далее информационное письмо о внесении изменений распечатывается на бланке Организации, подписывается руководителем Организации и направляется заказным письмом в Управление Роскомнадзора по Центральному федеральному округу.

Уведомление о намерении осуществлять обработку ПДн (информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку ПДн) также может подаваться в Роскомнадзор только в бумажном виде. В этом случае уведомление (информационное письмо) заполняется по форме, установленной приказом Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения».

Необходимо обратить внимание, что предоставляемые в Роскомнадзор сведения об обработке ПДн не должны противоречить сведениям, содержащимся в опубликованной (находящейся в открытом доступе) Политике оператора в отношении обработки ПДн, а также принятых локальных актах Организации, касающихся обработки и безопасности ПДн.

Организация обязана на постоянной основе приводить в соответствие сведения, представленные в Роскомнадзор, при изменениях в организационно-распорядительных и нормативных, методических документах, в том числе, в части изменений порядка и условий обработки ПДн, обеспечения их безопасности и т.д.

5 Организационные и технические меры, направленные на обеспечение безопасности ПДн при их обработке в информационных системах

Меры по обеспечению безопасности ПДн реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации

от 1 ноября 2012 г. № 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности ПДн.

Меры по обеспечению безопасности ПДн при их обработке в государственных информационных системах принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, установленными приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Рекомендации по порядку обеспечения защиты информации в государственных информационных системах описаны в Методических рекомендациях по обеспечению защиты информации в государственных информационных системах.

В общем случае при построении системы защиты ПДн проводятся следующие работы:

- формирование требований по обеспечению безопасности ПДн:
  - определение угроз безопасности ПДн при их обработке в ИСПДн;
  - определение уровня защищенности ПДн при их обработке в ИСПДн;
  - определение требований (мер) по обеспечению безопасности ПДн;
- разработка и внедрение организационно-технических решений на систему защиты ПДн;
- оценка соответствия ИСПДн требованиям по безопасности информации.

5.1 Определение угроз безопасности персональных данных

Для каждой ИСПДн Организации должны быть определены актуальные угрозы безопасности ПДн – разработана и утверждена модель угроз безопасности информации.

При разработке моделей угроз безопасности ПДн рекомендуется осуществлять с учетом положений нормативного правового акта[1] «Об утверждении перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

5.2 Определение уровня защищенности персональных данных при их обработке в информационной системе персональных данных

Определение уровня защищенности ПДн проводится на основании постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» с учетом данных, полученных при сборе исходных данных, и модели угроз безопасности ПДн.

[1] На момент написания настоящих Методических рекомендация указанный НПА согласован ФСТЭК России и ФСБ России и находится на стадии согласования в Правительстве Москвы.

Для определения уровня защищенности ПДн, обрабатываемых в ИСПДн, необходимо:

1. Определить тип угроз, актуальных для ИСПДн.
2. Определить категории ПДн, обрабатываемые в ИСПДн.
3. Определить тип субъектов ПДн.
4. Определить количество субъектов ПДн, данные которых обрабатываются в ИСПДн.
5. На основании данных, полученных на предыдущих этапах, сделать вывод об уровне защищенности ПДн, обрабатываемых в ИСПДн.

Определение типа угроз, актуальных для ИСПДн

В «Требованиях к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119, определены три типа угроз для ИСПДн:

- **угрозы 1-го типа** – если для ИСПДн в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе;
- **угрозы 2-го типа** – если для ИСПДн в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе;
- **угрозы 3-го типа** – если для ИСПДн актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности ПДн, актуальных для ИСПДн, должно производиться с учетом оценки возможного вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ «О персональных данных».

Определение категорий ПДн, обрабатываемых в ИСПДн

В соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119, вводятся следующие категории ПДн:

1) **специальные** категории ПДн – ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн;

2) **биометрические** ПДн – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн, и не относятся к специальным категориям ПДн;

3) **общедоступные** ПДн – ПДн субъектов ПДн, полученные только из общедоступных источников персональных данных, созданных в соответствии со ст. 8 ФЗ «О персональных данных»;

4) **иные** категории ПДн – ПДн, не относящиеся к специальным категориям ПДн, биометрическим ПДн и общедоступным ПДн.

Определение типа субъекта ПДн

В соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119, определены два типа субъектов ПДн:

- субъект ПДн, **являющийся сотрудником** оператора (Организации);
- субъект ПДн, **не являющийся сотрудником** оператора (Организации).

Определение количества субъектов ПДн, данные которых обрабатываются в ИСПДн

В соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119, пороговым значением для определения уровня защищенности ПДн, обрабатываемых в ИСПДн, является значение 100 000 субъектов ПДн, данные которых обрабатываемых в ИСПДн.

Определение уровня защищенности ПДн при их обработке в ИСПДн

Уровень защищенности ПДн при их обработке в ИСПДн определяется в соответствии с таблицей, приведенная ниже.

	Категории ПДн, количество субъектов ПДн, тип угроз											
	Специальные категории ПДн			Биометрические ПДн			Общедоступные ПДн			Иные категории ПДн		
Угрозы	>100 000	<100 000	сотр уд	>100 000	<100 000	сотр уд	>100 000	<100 000	сотр уд	>100 000	<100 000	сотр уд
1 тип	1УЗ			1УЗ			2УЗ			1УЗ		
2 тип	1УЗ	2УЗ		2УЗ			2УЗ	3УЗ		2УЗ	3УЗ	
3 тип	2УЗ	3УЗ		3УЗ			4УЗ			3УЗ	4УЗ	

Определение уровней защищенности ПДн при их обработке в ИСПДн проводится назначаемой приказом по Организации комиссии по классификации.

Результатом проведения классификации является присвоение ПДн при их обработке в ИСПДн соответствующего уровня защищенности и его документальное оформление.

5.3 Определение требований (мер) по обеспечению безопасности персональных данных

Состав и содержание мер по обеспечению безопасности ПДн для соответствующего уровня защищенности определены в приказе ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Выбор мер по обеспечению безопасности ПДн, подлежащих реализации в ИСПДн в рамках системы защиты информации, включает:

– определение базового набора мер по обеспечению безопасности ПДн для установленного уровня защищенности ПДн в соответствии с базовыми наборами мер по обеспечению безопасности ПДн, приведенными в приложении к «Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденному приказом ФСТЭК России от 18 февраля 2013 г. №21;

– адаптацию базового набора мер по обеспечению безопасности персона ПДн с учетом структурно-функциональных характеристик ИСПДн, информационных технологий, особенностей функционирования ИСПДн (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в ИСПДн, или структурно-функциональными характеристиками, не свойственными ИСПДн);

– уточнение адаптированного базового набора мер по обеспечению безопасности ПДн с учетом не выбранных ранее мер, приведенных в приложении к «Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденному приказом ФСТЭК России от 18 февраля 2013 г. №21, в результате чего определяются меры по обеспечению безопасности ПДн, направленные на нейтрализацию всех актуальных угроз безопасности ПДн для конкретной ИСПДн;

– дополнение уточненного адаптированного базового набора мер по обеспечению безопасности ПДн мерами, обеспечивающими выполнение требований к защите ПДн, установленными иными нормативными правовыми актами в области обеспечения безопасности ПДн и защиты информации.

5.4 Разработка и внедрение организационно-технических решений на систему защиты персональных данных

Разработка организационно-технических решений на систему защиты ПДн включает:

– проектирование системы защиты (выбор средств защиты и определение необходимых мер);

– разработка рабочей и эксплуатационной документации, организационно-распорядительных документов;

– при необходимости, проведение макетирования и тестирования системы защиты ПДн.

Внедрение организационно-технических решений на систему защиты ПДн включает:

– закупку и поставку технических, программных и программно-технических средств защиты информации;

– установку и настройку средств защиты информации

– разработку организационно-распорядительных документов по защите информации и внедрение организационных мер защиты информации;

– проведение предварительных испытаний системы защиты ПДн;

– проведение опытной эксплуатации средств защиты информации в комплексе с другими техническими и программными средствами ИСПДн в целях проверки их работоспособности в составе ИСПДн и отработки технологического процесса обработки ПДн;

– анализ уязвимостей системных компонент ИСПДн и принятие мер по их устранению (при необходимости);

– проведение приемочных испытаний системы защиты ПДн.

Организации для выполнения перечисленных мероприятий могут привлекать сторонние организации, оказывающие соответствующие услуги и имеющие лицензии ФСТЭК России и ФСБ России на осуществление необходимых видов деятельности.

5.5 Оценка соответствия информационной системы персональных данных требованиям по безопасности информации

До приемки ИСПДн в промышленную эксплуатацию должна быть проведена оценка соответствия ИСПДн на соответствие требованиям по безопасности информации. Оценка соответствия в виде аттестации проводится в обязательном порядке для государственных информационных систем, в которых обрабатываются ПДн.

6 Контроль соответствия обработки персональных данных требованиям законодательства в области обработки и защиты персональных данных

Контроль соответствия обработки ПДн требованиям законодательства в области обработки и защиты ПДн (далее – контроль) является неотъемлемой составной частью работ по обеспечению безопасности ПДн при создании и эксплуатации системы защиты ПДн.

Основными задачами контроля являются проверка соответствия принятых и принимаемых мер по защите информации требованиям внутренних документов Организации, требованиям нормативных правовых актов Российской Федерации,

города Москвы, проверка своевременности и полноты выполнения требований нормативных документов.

Контроль направлен на подтверждение того, что:

– обработка ПДн осуществляется в строгом соответствии с требованиями законодательства;

– созданная система защиты обеспечивает выполнение требований по защите информации при обработке ПДн;

– меры, средства и мероприятия, проводимые в целях защиты информации, соответствуют предъявляемым требованиям безопасности информации;

– средства защиты информации настроены и используются правильно;

– рекомендации предшествующего контроля реализованы.

Основными составляющими контроля могут быть:

– проверка корректности функционирования процессов обработки ПДн;

– проверка знания и выполнения работниками Организации требований по обработке и защите ПДн;

– проверка правильности и полноты выполняемых организационных и технических мероприятий по защите ПДн;

– автоматизированный контроль на основе мониторинга событий информационной безопасности;

– анализ защищенности информации, обрабатываемой в ИСПДн, с использованием специализированных средств и систем;

– проверка своевременности внесения изменений в проектную, эксплуатационную и организационно-распорядительную документацию по обеспечению безопасности ПДн;

– принятие на основании результатов контроля мер по устранению последствий нарушений требований по обеспечению безопасности ПДн.

Проведение контроля осуществляется на плановой основе, также возможно проведение внеплановых контрольных мероприятий. Порядок проведения контроля определяется организационно-распорядительными документами Организации.

Контроль может проводиться Организацией как самостоятельно, так и с привлечением юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Приложение 1 (справочное)
к Методическим рекомендациям
Основания для разработки организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных

Основания для разработки организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных

Основания необходимости разработки организационно-распорядительных документов в области обработки и обеспечения безопасности ПДн в соответствии с действующими нормативными правовыми актами Российской Федерации приведены в таблице ниже (Таблица 3).

Таблица 3 – Перечень организационно-распорядительных документов с указанием оснований для их разработки

№	Наименование документов	Нормы законодательства, устанавливающие обязательность наличия документов
1.	Политика в отношении обработки персональных данных	**Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:** **п.2 ч.1 ст.18.1** – Издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных … **Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»:** **п.2 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» (далее – Перечень)** – Документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.
2.	Правила обработки персональных данных,	**Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:** **п. 2 ч.1 ст.18.1** – Издание оператором… локальных актов по вопросам обработки персональных данных… **п.2 ч.1 ст.18.1** – Издание оператором… локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений… **п.5 ч.1 ст.18.1** – Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом. **п.6 ч.1 ст.18.1** – Ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику

		оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников. **Трудовой кодекс Российской Федерации от 20 декабря 2001 г. № 197-ФЗ** **ст. 87 -** Порядок хранения и использования персональных данных работников устанавливается работодателем с соблюдением требований настоящего Кодекса и иных федеральных законов. **ст.89** – «В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на: полную информацию об их персональных данных и обработке этих данных;…» **Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»:** **пп.«б» п.1 Перечня: «**– правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований». **пп.«б» п.1 Перечня:** «– типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей». **пп. «е» п.1 Перечня** – «осуществляют ознакомление служащих государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) организуют обучение указанных служащих.» **Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»:** **п.3 «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее – Положение)** – «Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными

№	Наименование документов	Нормы законодательства, устанавливающие обязательность наличия документов
		правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований настоящего Положения». **п.6 Положения** – «Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии)». **п.13 Положения** – «Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ».
3.	Правила рассмотрения запросов субъектов персональных данных или их представителей	**Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:** **ч.1 ст.14** – Субъект персональных данных имеет право на получение сведений, указанных в части 7 настоящей статьи, за исключением случаев, предусмотренных частью 8 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения его 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. **ч.4 ст.14** – В случае, если сведения, указанные в части 7 настоящей статьи, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом,

№	Наименование документов	Нормы законодательства, устанавливающие обязательность наличия документов
		принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных. **ч.5 ст.14** – Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 настоящей статьи, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 3 настоящей статьи, должен содержать обоснование направления повторного запроса. **ч.7 ст.14** - Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных,… **ст.21** Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных. **Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»:** **пп.«б» п.1 Перечня:** «– правила рассмотрения запросов субъектов персональных данных или их представителей».
4.	Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных	**Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:** **п.4 ч.1 ст.18.1** - Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора. **п.9 ч.2 ст.19** – «контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных». **Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним**

№	Наименование документов	Нормы законодательства, устанавливающие обязательность наличия документов
		нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»: **пп. «б» п.1 Перечня: «**– правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора» **пп. «д» п.1 Перечня: «**В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуют проведение периодических проверок условий обработки персональных данных в государственном или муниципальном органе.»
5.	Правила работы с обезличенными данными	**Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»:** **пп. «б» п.1 Перечня: «**– правила работы с обезличенными данными в случае обезличивания персональных данных» **пп. «з» п.1 Перечня** – «в случаях, установленных нормативными правовыми актами Российской Федерации, в соответствии с требованиями и методами, установленными уполномоченным органом по защите прав субъектов персональных данных, осуществляют обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ»
6.	Перечень должностей работников, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных	**Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним**

№	Наименование документов	Нормы законодательства, устанавливающие обязательность наличия документов
		нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»: **пп. «б» п.1 Перечня: «**– перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных»
7.	Перечень информационных систем	**Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»:** **пп. «б» п.1 Перечня: «**– перечень информационных систем персональных данных»
8.	Перечень персональных данных	**Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:** **ч.2 ст.5 -** Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. **ч.4 ст.5** – Обработке подлежат только персональные данные, которые отвечают целям их обработки. **ч.5 ст.5** – Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки. **ч.6 ст.5** – При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных. **ч.7 ст.5** – Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей

№	Наименование документов	Нормы законодательства, устанавливающие обязательность наличия документов
		обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. **Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»:** **пп.«б» п.1 Перечня: «**– перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных услуг и осуществления государственных или муниципальных функций»
9.	Перечень должностей работников, замещение которых предусматривает осуществление обработки персональных данных	**Трудовой кодекс Российской Федерации от 20 декабря 2001 г. № 197-ФЗ** **ст. 88 При передаче персональных данных работника работодатель должен соблюдать следующие требования: …** «разрешать доступ к персональным данным работника только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций.» **Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»:** **п. 13 Положения** – «Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.» **Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»:**

№	Наименование документов	Нормы законодательства, устанавливающие обязательность наличия документов
		пп.«б» п.1 Перечня: «– перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным». **Постановление Правительства Российской Федерации от 01 ноября 2012 г № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:** **пп.«в» п.13 Требований к защите персональных данных при их обработке в информационных системах персональных данных** – «Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований: в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.» **Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»:** **пп. «в» п.5 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности** (далее - Меры) – утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей. **пп. «а», «б» п.8 Мер– «**Для выполнения требования, указанного в подпункте «в» пункта 5 настоящего документа, необходимо: а) разработать и утвердить документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

№	Наименование документов	Нормы законодательства, устанавливающие обязательность наличия документов
		б) поддерживать в актуальном состоянии документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей»
10.	Перечень мест хранения материальных носителей персональных данных	**Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»:** **п.13 Положения: «**Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.»
11.	Должностные обязанности ответственного за организацию обработки персональных данных	**Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:** **п.1 ч.1 ст.18.1 – «**назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;» **ч.1 ст.22.1 –** Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных. **Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»:** **пп. «б» п.1 Перечня:** «- должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных в государственном или муниципальном органе».
12.	Обязательство о неразглашении и обеспечении	**Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:**

№	Наименование документов	Нормы законодательства, устанавливающие обязательность наличия документов
	безопасности персональных данных	**ст. 7 –** Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
13.	Типовое обязательство работника о прекращении обработки персональных данных в случае расторжения с ним трудового договора	**Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»:** **пп. «б» п.1 Перечня:** «- типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей».
14.	Типовая форма согласия на обработку персональных данных работника	**Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»:** **пп. «б» п.1 Перечня:** «– типовая форма согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные»
15.	Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные	**Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:** **ч.2 ст.18 -** Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные **Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных**

№	Наименование документов	Нормы законодательства, устанавливающие обязательность наличия документов
		Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»: **пп. «б» п.1 Перечня: «**– типовая форма согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные»
16.	Порядок доступа в помещения, в которых ведется обработка персональных данных	**Постановление Правительства Российской Федерации от 01 ноября 2012 г № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:** **пп.«в» п.13 Требований к защите персональных данных при их обработке в информационных системах персональных данных** – «Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований: в) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;» **Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»:** **п.8 Положения: «**При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия: а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;»

№	Наименование документов	Нормы законодательства, устанавливающие обязательность наличия документов
		Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»: **пп. «а» п.5 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности** – организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения. **пп. «б» п.6 Мер– «**Для выполнения требования, указанного в подпункте «а» пункта 5 настоящего документа, необходимо…: б) утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях».

Приложение 13 (справочное)
к Методическим рекомендациям
Ответственность за нарушение порядка обработки и обеспечения безопасности персональных данных

Ответственность за нарушение порядка обработки и обеспечения безопасности персональных данных

1. Дисциплинарная ответственность

Согласно статье 24 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», лица, виновные в нарушении требований Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

Согласно статье 90 Трудового кодекса Российской Федерации от 20 декабря 2001г. № 197-ФЗ, лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Статьей 81 Трудового кодекса Российской Федерации от 20 декабря 2001 г. № 197-ФЗ предусмотрено расторжение трудового договора в случае разглашения работником персональных данных, ставших известными работнику в связи с исполнением им трудовых обязанностей.

Виды дисциплинарных взысканий, порядок их применения и снятия устанавливаются главой 30 Трудового кодекса Российской Федерации от 20 декабря 2001г. № 197-ФЗ РФ и правилами внутреннего трудового распорядка Организации.

2. Административная ответственность

К административной ответственности за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) могут привлекаться как сама Организация, так и конкретные работники, исполняющие соответствующие трудовые обязанности.

Лица, виновные в нарушении правил обработки персональных данных, могут привлекаться к административной ответственности по следующим основаниям, приведенным в таблице 1.

Таблица 1 – Административная ответственность

Статья КоАП РФ[2]	Вид нарушения	Субъект нарушения	Ответственность
ст. 13.11, ч.1	Обработка ПДн в случаях, не предусмотренных законодательством Российской Федерации в области ПДн, либо обработка ПДн, несовместимая с целями сбора ПДн (за исключением случаев, предусмотренных ч.2 ст.13.11), если эти действия не содержат уголовно наказуемого деяния	Гражданин	Предупреждение или наложение административного штрафа в размере от 1000 до 3000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 5000 до 10 000 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 30 000 до 50 000 рублей
ст. 13.11, ч.2	Обработка ПДн без согласия в письменной форме субъекта ПДн на обработку его ПДн в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области ПДн, если эти действия не содержат уголовно наказуемого деяния, либо обработка ПДн с нарушением установленных законодательством Российской Федерации в области ПДн требований к составу сведений, включаемых в согласие в письменной форме субъекта ПДн на обработку его ПДн	Гражданин	Наложение административного штрафа в размере от 3000 до 5000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 10 000 до 20 000 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 15 000 до 75 000 рублей
ст. 13.11, ч.3	Невыполнение оператором предусмотренной законодательством Российской Федерации в области ПДн обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки ПДн, или сведениям о реализуемых требованиях к защите ПДн	Гражданин	Предупреждение или наложение административного штрафа в размере от 700 до 1 500 рублей
		Должностное лицо	Наложение административного штрафа в размере от 3000 до 6000 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 15 000 до 30 000 рублей

[2] Кодекс Российской Федерации об административных правонарушениях от 31 декабря 2001 г. № 195-ФЗ

Статья КоАП РФ[2]	Вид нарушения	Субъект нарушения	Ответственность
ст. 13.11, ч.4	Невыполнение оператором предусмотренной законодательством Российской Федерации в области ПДн обязанности по предоставлению субъекту ПДн информации, касающейся обработки его ПДн	Гражданин	Предупреждение или наложение административного штрафа в размере от 1000 до 2000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 4000 до 6000 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 20 000 до 40 000 рублей
ст. 13.11, ч.5	Невыполнение оператором в сроки, установленные законодательством Российской Федерации в области ПДн, требования субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн об уточнении ПДн, их блокировании или уничтожении в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки	Гражданин	Предупреждение или наложение административного штрафа в размере от 1000 до 2000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 4000 до 10 000 рублей;
		Юридическое лицо	Наложение административного штрафа в размере от 25 000 тысяч до 45 000 рублей
ст. 13.11, ч.6	Невыполнение оператором при обработке ПДн без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством Российской Федерации в области ПДн сохранность ПДн при хранении материальных носителей ПДн и исключающих НСД, если это повлекло неправомерный или случайный доступ к ПДн, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении ПДн, при отсутствии признаков уголовно наказуемого деяния	Гражданин	Наложение административного штрафа в размере в размере от 700 до 2000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 4000 до 10 000 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 25 000 тысяч до 50 000 рублей
ст. 13.11, ч.7	Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной	Должностное лицо	Предупреждение или наложение административного

Статья КоАП РФ[2]	Вид нарушения	Субъект нарушения	Ответственность
	законодательством Российской Федерации в области ПДн обязанности по обезличиванию ПДн либо несоблюдение установленных требований или методов по обезличиванию ПДн		штрафа в размере от 3000 до 6000 рублей
ст. 13.12, ч. 6	Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных частями 1, 2 и 5 ст. 13.12 КоАП	Гражданин	Наложение административного штрафа в размере от 500 до 1000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 1000 до 2000 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 10 000 до 15 000 рублей
ст. 13.14	Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 КоАП	Гражданин	Наложение административного штрафа в размере от 500 до 1000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 4000 до 5000 рублей
ст. 19.4, ч. 1	Неповиновение законному распоряжению или требованию должностного лица органа, осуществляющего государственный надзор (контроль), муниципальный контроль	Гражданин	Предупреждение или наложение административного штрафа в размере от 500 до 1000 рублей
		Должностное лицо	Наложение административного штрафа в размере от 2000 до 4000 рублей
ст. 19.5, ч. 1	Невыполнение в установленный срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), муниципальный контроль, об устранении нарушений законодательства	Гражданин	Наложение административного штрафа в размере от 300 до 500 рублей
		Должностное лицо	Наложение административного штрафа в размере от 1000 до 2000 рублей или

Статья КоАП РФ[2]	Вид нарушения	Субъект нарушения	Ответственность
			дисквалификация на срок до трех лет
		Юридическое лицо	Наложение административного штрафа в размере от 10 000 до 20 000 рублей
ст. 19.7	Непредставление или несвоевременное представление в государственный орган (должностному лицу), орган (должностному лицу), осуществляющий (осуществляющему) государственный контроль (надзор), муниципальный контроль, сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, либо представление в государственный орган (должностному лицу), орган (должностному лицу), осуществляющий (осуществляющему) государственный контроль (надзор), муниципальный контроль, таких сведений (информации) в неполном объеме или в искаженном виде, за исключением случаев, предусмотренных ст. 6.16, ч.2 ст.6.31, ч.. 1, 2 и 4 ст. 8.28.1, ст.8.32.1, ч.5 ст.14.5, ч.2 ст.6.31, ч.4 ст.14.28, ч.1 ст.14.46.2, ст.19.7.1, 19.7.2, 19.7.2-1, 19.7.3, 19.7.5, 19.7.5-1, 19.7.5-2, 19.7.7, 19.7.8, 19.7.9, 19.7.12, 19.7.13, 19.7.14, 19.8, 19.8.3 КоАП	Гражданин	Предупреждение или наложение административного штрафа в размере от 100 до 300 рублей
		Должностное лицо	Наложение административного штрафа в размере от 300 до 500 рублей
		Юридическое лицо	Наложение административного штрафа в размере от 3000 до 5000 рублей

3. Уголовная ответственность

Уголовная ответственность за нарушение правил работы с ПДн может наступить в случаях, указанных в таблице 2.

Таблица 2– Уголовная ответственность

Статья УК РФ	Вид нарушения	Ответственность
ст. 137, ч. 1	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или	Штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо обязательными работами на срок до 360 часов,

Статья УК РФ	Вид нарушения	Ответственность
	семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации	либо исправительными работами на срок до 1 года, либо принудительными работами на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового, либо арестом на срок до 4 месяцев, либо лишением свободы на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет
ст. 137, ч. 2	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, совершенные лицом с использованием своего служебного положения	Штраф в размере от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 2 лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, либо принудительными работами на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового, либо арестом на срок до 6 месяцев, либо лишением свободы на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет
ст. 137, ч. 3	Незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия	Штраф в размере от 150 000 до 350 000 рублей или в размере заработной платы или иного дохода осужденного за период от 18 месяцев до 3 лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 3 до 5 лет, либо принудительными работами на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет или без такового, либо арестом на срок до 6 месяцев, либо лишением свободы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 6 лет
ст. 272, ч. 1	Неправомерный доступ к охраняемой законом компьютерной информации, если	Штраф в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо

Статья УК РФ	Вид нарушения	Ответственность
	это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации	исправительными работами на срок до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы на тот же срок
ст. 272, ч. 2	Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб или совершенное из корыстной заинтересованности	Штраф в размере от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 2 лет, либо исправительными работами на срок от 1 года до 2 лет, либо ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 4 лет, либо лишением свободы на тот же срок
ст. 272, ч. 3	Деяния, предусмотренные ч.1-2 ст. 272 УК РФ, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения	Штраф в размере до 500 000 рублей или в размере заработной платы или иного дохода осужденного за период до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 5 лет, либо лишением свободы на тот же срок
ст. 272, ч. 4	Деяния, предусмотренные ч. 1-3 ст. 272 УК РФ, если они повлекли тяжкие последствия или создали угрозу их наступления	Лишение свободы на срок до семи лет
ст. 273, ч. 1	Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации	Ограничение свободы на срок до 4 лет, либо принудительные работы на срок до 4 лет, либо лишение свободы на тот же срок со штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев
ст. 273, ч. 2	Деяния, предусмотренные ч. 1 ст. 273, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности	Ограничение свободы на срок до 4 лет, либо принудительные работы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового, либо лишением свободы на срок до 5 лет со штрафом в размере от 100 000 до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период от 2 до 3 лет или без такового и с лишением права

Статья УК РФ	Вид нарушения	Ответственность
		занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового
ст. 273, ч. 3	Деяния, ч. 1-2 ст. 273, если они повлекли тяжкие последствия или создали угрозу их наступления	Лишение свободы на срок до семи лет
ст. 274, ч. 1	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб	Штраф в размере до 500 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо исправительными работами на срок от 6 месяцев до 1 года, либо ограничением свободы на срок до 2 лет, либо принудительными работами на срок до 2 лет, либо лишением свободы на тот же срок
ст. 274, ч. 2	Деяние, предусмотренное ч.1 ст. 274, если оно повлекло тяжкие последствия или создало угрозу их наступления	Принудительные работы на срок до 5 лет либо лишением свободы на тот же срок

4.Гражданско-правовая ответственность

Порядок защиты нематериальных благ, к числу которых относятся честь и доброе имя, деловая репутация; неприкосновенность частной жизни; личная и семейная тайна определяется Гражданским кодексом Российской Федерации и иными законами.