

Титульный лист

«Принято»

Решением Учёного совета ОмГПУ
протокол № 1
от « 23 » сентября 2011 г.

«Утверждено»

Приказом и.о. ректора ФГБОУ ВПО «ОмГПУ»
№ 01-04/261 от « 30 » сентября 2011 г.

И.о. ректора ФГБОУ ВПО «ОмГПУ»



И.М. Щеткин

ПОЛОЖЕНИЕ О ПЕРСОНАЛЬНЫХ ДАННЫХ
в федеральном государственном бюджетном образовательном учреждении
высшего профессионального образования
«Омский государственный педагогический университет»

Оглавление

Титульный лист	1
Оглавление.....	2
1. Аннотация.....	6
2. Положение о персональных данных.....	6
2.1. Назначение Положения	6
2.2. Порядок утверждения Положения.....	6
2.3. Идентификация Положения.....	6
2.4. Публикация Положения.....	6
2.5. Ознакомление должностных лиц учреждения с Положением.....	6
2.6. Нормативно-правовое обоснование и статус Положения.....	6
2.7. Срок действия Положения.....	6
2.8. Толкование Положения и порядок его применения.....	6
3. Общие требования по обработке персональных данных.....	7
3.1. Понятия и определения.....	7
3.2. Принципы обработки персональных данных	7
3.3. Цель обработки персональных данных.....	8
3.4. Способы обработки персональных данных в информационных системах персональных данных в зависимости от применения средств автоматизации.....	8
3.4.1. Правила обработки персональных данных без использования средств автоматизации.....	8
3.4.2. Правила обработки персональных данных средствами автоматизации.....	9
3.4.3. Правила исключительно автоматизированной обработки персональных данных	10
3.4.4. Правила смешанной обработки персональных данных	10
3.5. Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от категории обрабатываемых персональных данных.....	10
3.5.1. Правила обработки специальных категорий персональных данных.....	10
3.5.2. Правила обработки биометрических персональных данных	11
3.5.3. Правила обработки общедоступных персональных данных	11
3.5.4. Правила обработки персональных данных, не относящихся к особым категориям.....	11
3.6. Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от цели обработки персональных данных.....	12
3.6.1. Правила обработки персональных данных с целью однократного пропуска субъекта персональных данных на охраняемую территорию	12
3.6.2. Правила обработки персональных данных при трансграничной передаче персональных данных.....	12
3.6.3. Правила при поручении обработки персональных данных другому оператору персональных данных.....	12
3.6.4. Обезличивание персональных данных	12
3.6.5. Правила обработки персональных данных в целях продвижения товаров, работ, услуг на рынке	13
3.7. Необходимость обработки персональных данных	13
3.8. Перечни идентификаторов персональных данных, используемые для решения задач и функций структурными подразделениями.....	13
3.9. Правовое основание обработки персональных данных	13
3.9.1. Определение законности целей обработки персональных данных	13
3.9.2. Юридические последствия, порождаемые в результате действий (операций) с персональными данными, в отношении субъекта персональных	

данных либо иным образом затрагивающих права и свободы субъекта персональных данных.....	14
3.9.3. Заданные характеристики безопасности персональных данных	14
3.9.4. Определение сроков обработки, в том числе хранения персональных данных	15
3.9.5. Контроль за соблюдением сроков обработки персональных данных и фактов достижения целей обработки персональных данных	16
3.10. Действия (операции) с персональными данными;.....	16
3.10.1. Способы сбора персональных данных и источники их получения	16
3.10.2. Способы и правила систематизации, накопления, уточнения и использования персональных данных.....	17
3.10.3. Способы обозначения документов содержащих персональные данные ...	18
3.10.4. Способы передачи персональных данных и их получатели.....	18
3.10.5. Хранение персональных данных.....	19
3.10.6. Способы и порядок блокирования персональных данных.....	20
3.10.7. Способы и порядок уничтожения персональных данных	20
3.11. Круг субъектов, персональные данные которых подлежат обработке	21
3.12. Перечень должностных лиц, осуществляющих обработку персональных данных	21
3.13. Права и обязанности при обработке персональных данных.....	21
3.13.1. Права и обязанности субъекта персональных данных.....	21
3.13.2. Права и обязанности ОУ при обработке персональных данных субъектов персональных данных.....	22
3.14. Порядок взаимодействия с субъектами персональных данных	23
3.14.1. Установленные сроки выполнения действий по защите прав субъектов персональных данных.....	23
3.14.2. Требования по уведомлениям субъектов персональных данных и в иных случаях	24
3.14.3. Порядок разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав.....	24
3.14.4. Порядок реагирования на обращения субъектов персональных данных	25
3.14.5. Порядок действий при обращениях субъектов персональных данных	25
3.14.6. Порядок действий при достижении целей обработки персональных данных и отзыве согласия на обработку персональных данных.....	27
3.14.7. Порядок действий при отзыве согласия субъекта персональных данных на обработку его персональных данных.....	27
3.15. Согласие субъекта персональных данных на обработку его персональных данных	27
3.16. Уведомление об обработке (о намерении осуществлять обработку) персональных данных.....	29
4. Организация обработки персональных данных в ОУ.....	30
4.1. Организационная структура и функции ОУ.....	30
4.2. Задачи и функции подразделений.....	30
4.3. Направления обработки персональных данных в ОУ.....	30
4.3.1. Обработка персональных данных в рамках деятельности ОУ в качестве образовательного учреждения.....	30
4.3.2. Обработка персональных данных в рамках деятельности ОУ в качестве работодателя	30
4.3.3. Обработка персональных данных в рамках деятельности в качестве собственника имущества.....	31
4.4. Информационные системы персональных данных.....	31
4.4.1. Критерии определения информационных систем персональных данных в	

ОУ	31
4.4.2. Наименование информационной системы персональных данных	32
4.4.3. Цели создания или эксплуатации информационной системы персональных данных	32
4.4.4. Параметры, характеризующие информационную систему персональных данных	32
4.5. Юридический паспорт информационной системы персональных данных.....	33
4.6. Порядок создания, модернизации и ликвидации информационных систем персональных данных в ОУ	34
4.6.1. Порядок создания информационных систем персональных данных в ОУ..	34
4.6.2. Порядок модернизации информационных систем персональных данных в ОУ	34
4.6.3. Порядок ликвидации информационных систем персональных данных в ОУ	34
4.7. Перечень информационных систем персональных данных в ОУ	34
5. Конфиденциальность персональных данных.....	35
5.1. Режим ограниченного доступа к персональным данным в ОУ	35
5.2. Порядок учета и маркирования материальных носителей информации, образующихся в процессе обработки персональных данных.....	36
5.3. Порядок снятия режима конфиденциальности.....	36
6. Обеспечение безопасности персональных данных при их обработке	37
6.1. Принципы обеспечения безопасности персональных данных при их обработке.....	37
6.2. Требования по уровню обеспечения безопасности	37
6.3. Состав мероприятий по обеспечению безопасности персональных данных.....	38
6.3.1. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.....	38
6.3.2. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой с использованием средств автоматизации.....	38
6.4. Система защиты персональных данных	41
6.4.1. Частные модели угроз и нарушителя	41
6.4.2. Средства защиты информации.....	42
6.5. Требования к помещениям, в которых производится обработка персональных данных.....	42
6.6. Требования к содержанию организационных мероприятий по обеспечению безопасности	43
6.7. Требования к персоналу, задействованному в обработке персональных данных.....	43
6.8. Требования к порядку передачи (пересылки) носителей информации, содержащих персональные данные.....	43
6.9. Требования к техническим средствам, системному программному обеспечению и их настройкам	43
6.10. Регламент оценки соответствия требованиям по безопасности информации	43
7. Порядок контроля за соблюдением требований по обработке и обеспечению безопасности персональных данных.....	44
7.1. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности данных.....	44
7.2. Порядок внешнего контроля за соблюдением требований по обработке и обеспечению безопасности данных.....	44
8. Ответственность за нарушение норм, регулирующих обработку персональных данных.....	45
9. Мероприятия при возникновении обстоятельств непреодолимой силы (форс-	

мажор).....	45
10. Мероприятия по обработке персональных данных при ликвидации или реорганизации ОУ	45
11. Приложения.....	45
Приложение 1. Перечень документов по разработке Положения о персональных данных в ОУ	47
Приложение 2. Форма юридического паспорта информационной системы персональных данных.....	53
Приложение 3. Форма перечня информационных систем персональных данных	67
Приложение 4. Форма согласия на обработку персональных данных.....	69
Приложение 5. Форма согласия субъекта персональных данных на запрос его персональных данных у третьих лиц	73
Приложение 6. Форма журнала учета лиц (организаций), получивших доступ к персональным данным, и (или) лиц (организаций), которым такая информация была предоставлена или передана	74
Приложение 7. Форма акта уничтожения персональных данных субъектов персональных данных по достижении цели обработки, внесения изменений, блокировки и т.д.....	75
Приложение 8. Форма уведомлений о совершенных операциях над персональными данными.....	76
Приложение 9. Содержание дополнений к договорам с физическими лицами по вопросам обработки персональных данных	76

1. Аннотация

Настоящим Положением о персональных данных (далее – Положение) регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральным государственным бюджетным образовательным учреждением высшего профессионального образования «Омский государственный педагогический университет» (далее – ОУ) с использованием средств автоматизации или без использования таких средств.

2. Положение о персональных данных

2.1. Назначение Положения

Настоящее Положение предназначено для определения правил обработки и обеспечения безопасности персональных данных с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также законных прав и интересов ОУ связанных с необходимостью обработки персональных данных.

Все работы по обработке персональных данных в ОУ должны проводиться в строгом соответствии с настоящим Положением.

2.2. Порядок утверждения Положения

Настоящее Положение принимается Ученым советом ОУ, утверждается и вводится в действие приказом ректора (далее – Руководитель) ОУ и является обязательным для исполнения всеми работниками.

2.3. Идентификация Положения

Полное и официальное наименование настоящего Положения: «Положение о персональных данных в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Омский государственный педагогический университет».

Полное наименование настоящего Положения является однозначно определяющим его идентификатором.

2.4. Публикация Положения

Настоящее Положение является внутренним документом ОУ и не подлежит публикации в полном объеме.

С целью ознакомления заинтересованных лиц с отдельными положениями настоящего Положения из него осуществляется выписки. Допускается публикация выписок из настоящего Положения (в том числе и на официальном сайте ОУ), после проведения проверочных мероприятий на предмет отсутствия в них информации ограниченного доступа.

2.5. Ознакомление должностных лиц учреждения с Положением

Все должностные лица ОУ обязаны ознакомиться с настоящим Положением под роспись.

Допуск к обработке персональных данных без ознакомления с настоящим Положением категорически запрещается.

2.6. Нормативно-правовое обоснование и статус Положения

Настоящее Положение разработано в соответствии с действующим законодательством Российской Федерации, государственными и отраслевыми стандартами, рекомендациями уполномоченных органов исполнительной власти и др. (Приложение 1), и является основным документом, определяющим общие правила обработки и обеспечения безопасности персональных данных в ОУ.

2.7. Срок действия Положения

Действие настоящего Положения является бессрочным.

2.8. Толкование Положения и порядок его применения

Термины, применяемые в настоящем Положении, используются строго в контексте общего смысла Положения. В случае противоречия и (или) расхождения смысла и толкования положений настоящего Положения со смыслом терминов и определений, приведенных в п. 3.1, применяется толкование терминов и определений в соответствии с п. 3.1 настоящего Положения.

В случае противоречия и (или) расхождения названия какой-либо статьи настоящего Положения со

смыслом какого-либо пункта, в ней содержащегося, подлежат применению формулировки каждого конкретного пункта.

В случае противоречия и (или) расхождения положений какого-либо приложения к настоящему Положению с положениями настоящего Положения подлежат применению формулировки положений настоящего Положения.

В случае противоречия и (или) расхождения положений настоящего Положения с действующим законодательством Российской Федерации, применяются положения соответствующих нормативно-правовых актов Российской Федерации.

В случае возникновения противоречий и (или) расхождений различных положений настоящего Положения применяются специальные положения.

3. Общие требования по обработке персональных данных

3.1. Понятия и определения

Термины, определения и понятия, используемые в настоящем Положении, определяются согласно нормативно-правовым актам и документам, приведенным в Приложении 1 к настоящему Положению.

3.2. Принципы обработки персональных данных

Обработка персональных данных в ОУ должна осуществляться на основе следующих принципов:

- соблюдения законных прав субъекта персональных данных;
- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям ОУ;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки;
- недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;
- обработки персональных данных (в том числе специальной категории и биометрических персональных данных) с письменного согласия субъектов персональных данных либо на ином законном основании;
- уничтожения персональных данных по достижении целей обработки или в случае утраты необходимости в их достижении;
- требования от организаций, которым поручается обработка персональных данных, соблюдения законодательства по обработке персональных данных;
- законности при осуществлении трансграничной передачи персональных данных;
- принятия на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы только с письменного согласия субъектов персональных данных либо на ином законном основании;
- принятия необходимых организационных и технических мер для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий;
- соблюдения обязанностей, возлагаемых на оператора персональных данных, действующим законодательством и иными нормативными актами по обработке персональных данных;
- запрета содержания в нормативных правовых актах по отдельным вопросам, касающимся обработки персональных данных, положений, ограничивающих права субъектов персональных данных;
- личной ответственности должностных лиц, осуществляющих обработку персональных данных;

- документального подтверждения всех принятых решений по обработке и обеспечению безопасности персональных данных.
- Нарушение указанных принципов обработки персональных данных запрещается.

3.3. Цель обработки персональных данных

ОУ, являясь оператором персональных данных, должно определять цели и содержание обработки персональных данных в своих информационных системах персональных данных и в учреждении в целом.

Цель обработки персональных данных в учреждении в целом, должна соответствовать заявленным в учредительных документах ОУ видам деятельности.

Цели обработки персональных данных в информационных системах персональных данных должны быть четко определены и соответствовать перечням задач или функций структурных подразделений (должностных лиц) ОУ, указанным в положениях о таких структурных подразделениях (должностных обязанностях).

Цели обработки персональных данных определяют:

- объем обрабатываемых персональных данных (достаточность и недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных);
- характер обрабатываемых персональных данных;
- способы обработки персональных данных;
- срок обработки (в том числе хранения) персональных данных.

Цели обработки персональных данных должны быть:

- законны (иметь правовое обоснование);
- заранее определены;
- заявлены при сборе персональных данных;
- соответствовать полномочиям ОУ;

Не допускается объединение созданных для несовместимых между собой целей баз данных информационных систем персональных данных

Совместимость целей определяется по наличию общей цели связанной с заявленным в учредительных документах ОУ видом деятельности или по наличию общей цели, определяемой действующим законодательством Российской Федерации.

3.4. Способы обработки персональных данных в информационных системах персональных данных в зависимости от применения средств автоматизации

Способы обработки персональных данных в рамках каждой из заявленных задач обработки персональных данных в информационной системе персональных данных:

- обработка персональных данных без использования средств автоматизации;
- обработка персональных данных с использованием средств автоматизации;
- исключительно автоматизированная обработка персональных данных;
- смешанная обработка персональных данных.

3.4.1. Правила обработки персональных данных без использования средств автоматизации

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых, заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности, при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных,

осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать: сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых, заведомо не совместимы.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

3.4.2. Правила обработки персональных данных средствами автоматизации

Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе, за исключением случаев, когда федеральными законами Российской Федерации предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных возлагается на ОУ.

Согласие субъекта персональных данных на обработку его персональных данных предоставляется (берется) только в письменной форме.

Допускается включение согласия в типовые формы (бланки) материальных носителей персональных данных и в договоры с субъектами персональных данных.

Для обработки персональных данных, содержащихся в согласии в письменной форме субъекта на обработку его персональных данных, дополнительного согласия не требуется

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

В случае получения согласия от законного представителя субъекта персональных данных или наследников субъекта персональных данных они обязаны предоставить документы, подтверждающие их полномочия.

Согласие на обработку персональных данных может быть отозвано субъектом персональных

данных путем направления обращения в ОУ. При получении такого обращения выполняются действия предусмотренные пунктом 3.14.7 настоящего Положения.

Согласия субъектов персональных данных должны храниться в ОУ.

Требования к содержанию согласия на обработку персональных данных приведено в разделе 3.15 настоящего Положения.

3.4.3. Правила исключительно автоматизированной обработки персональных данных

Решение, порождающее юридические последствия в отношении субъекта персональных данных, или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

В остальных случаях принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы запрещается.

К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы.

Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

3.4.4. Правила смешанной обработки персональных данных

При смешанной обработке персональных данных необходимо выполнять правила объединяющие правила обработки персональных данных при их обработке каждым из используемых при смешанной обработке персональных данных способов.

3.5. Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от категории обрабатываемых персональных данных

В ОУ устанавливаются следующие особые правила обработки персональных данных в зависимости от категории обрабатываемых персональных данных:

- обработка специальных категорий персональных данных;
- обработка биометрических персональных данных;
- обработка общедоступных персональных данных;
- обработка персональных данных, не входящих в указанные категории.

3.5.1. Правила обработки специальных категорий персональных данных

К специальным категориям персональных данных относятся сведения о:

- расовой принадлежности;
- национальной принадлежности;
- политических взглядах;
- религиозных убеждениях;
- философских убеждениях;
- состоянии здоровья;
- интимной жизни;
- судимости.

Разрешается обработка сведений о состоянии здоровья работника ОУ в объеме сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

Разрешается обработка сведений о состоянии здоровья учащегося ОУ в объеме сведений, которые относятся к вопросу об оказании ему образовательных услуг, а также охраны его здоровья в соответствии с действующим законодательством Российской Федерации.

Обработка специальных категорий персональных данных в остальных случаях в ОУ не

допускается.

3.5.2. Правила обработки биометрических персональных данных

К биометрическим персональным данным относятся сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, в том числе:

- данные изображения отпечатка пальца (информация об особенностях строения папиллярных узоров пальцев);
- данные контрольных точек отпечатка пальца;
- данные изображения лица;
- данные изображения радужной оболочки глаза;
- данные динамики подписи;
- данные изображения сосудистого русла;
- кодированная информация об определенных фрагментах дезоксирибонуклеиновой кислоты;
- данные об иных поведенческих, физиологических или биологических характеристиках.

Обработка биометрических персональных данных в ОУ осуществляется исключительно без использования средств автоматизации.

В случае принятия решения об обработке биометрических персональных данных, на основе которых можно установить личность человека, такие данные могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.

3.5.3. Правила обработки общедоступных персональных данных

К общедоступным персональным данным относятся персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Общедоступные персональные данные физических лиц в ОУ обрабатываются в исключительных случаях в сроки, не превышающие необходимые для их использования. При этом совместно с такими данными должны собираться реквизиты их источника и подтверждение согласия субъекта персональных данных на включение такой информации в общедоступные источники персональных данных, так как в случае обработки общедоступных персональных данных обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на ОУ. По достижении целей обработки общедоступных персональных данных они подлежат немедленному уничтожению.

Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

С целью информационного обеспечения и осуществления взаимодействия как внутри ОУ, так и со сторонними физическими и юридическими лицами в ОУ может создаваться общедоступный источник персональных данных.

В общедоступный источник персональных данных с письменного согласия субъекта персональных данных могут включаться: должность, фамилия, имя, отчество, абонентский номер рабочего телефона, место получения образования, достигнутые результаты и другая информация. Исключение персональных данных из указанного общедоступного источника осуществляется при утрате необходимости в обработке таких данных, либо на основании заявления субъекта персональных данных в установленном настоящим Положением (пункт 3.14.7) и действующим законодательством Российской Федерации порядке.

3.5.4. Правила обработки персональных данных, не относящихся к особым категориям

Обработка персональных данных, не относимых к особым категориям персональных данных, должна осуществляться на основании правил, инструкций, руководств, регламентов и иных документов, определяющих технологический процесс обработки информации, содержащих такие данные, определенный для выполнения конкретных операций с заранее определенными целями, с учетом требований настоящего Положения.

3.6. Особые правила обработки персональных данных в информационных системах персональных данных в зависимости от цели обработки персональных данных

В ОУ устанавливаются следующие особые правила обработки персональных данных в зависимости от цели обработки персональных данных:

- обработка персональных данных с целью однократного пропуска субъекта персональных данных на охраняемую территорию;
- обработка персональных данных при трансграничной передаче персональных данных;
- поручение обработки персональных данных другому оператору персональных данных;
- обезличивание персональных данных;
- обработка персональных данных в целях продвижения товаров, работ, услуг на рынке.

3.6.1. Правила обработки персональных данных с целью однократного пропуска субъекта персональных данных на охраняемую территорию

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию ОУ, должны соблюдаться следующие условия:

- 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;
- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

3.6.2. Правила обработки персональных данных при трансграничной передаче персональных данных

К трансграничной передаче персональных данных относится передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства

Трансграничная передача персональных данных в ОУ осуществляется только на основании:

- согласия в письменной форме субъекта персональных данных, предусматривающего такую передачу и оговаривающего условия ее осуществления;
- договора, стороной которого является субъект персональных данных, в котором оговорены условия осуществления такой передачи.

3.6.3. Правила при поручении обработки персональных данных другому оператору персональных данных

В случае если ОУ на основании договора (в том числе агентского) поручает обработку персональных данных другому оператору персональных данных, существенным условием договора должна являться обязанность обеспечения указанным оператором конфиденциальности персональных данных и безопасности персональных данных при их обработке.

При этом должны выполняться правила обработки персональных данных субъектов персональных данных при их передаче третьим лицам, установленные пунктом 3.10.4.1 настоящего Положения.

3.6.4. Обезличивание персональных данных

Под обезличиванием персональных данных понимаются действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обезличивание персональных данных в ОУ при обработке персональных данных с использованием средств автоматизации осуществляется с целью выполнения требований по предоставлению отчетности по результатам деятельности в соответствии с нормативными

документами органов государственной власти и управления.

Допускается обезличивание персональных данных при обработке персональных данных без использования средств автоматизации производимым способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.6.5. Правила обработки персональных данных в целях продвижения товаров, работ, услуг на рынке

Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи (например, для предложения приобретения учебных пособий, рекламы своего учебного учреждения и др.) допускается только при условии предварительного письменного согласия субъекта персональных данных.

ОУ обязано по требованию субъекта персональных данных немедленно прекратить обработку его персональных данных, осуществляемую в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи.

3.7. Необходимость обработки персональных данных

Необходимость обработки определенного набора персональных данных определяется заранее определенной и документированной целью обработки персональных данных и может устанавливаться (требоваться) нормативно-правовым актом (например, федеральным законом) или определяется принятым в ОУ порядком выполнения определенных операций по обработке информации, в рамках заявленных в учредительных документах ОУ видов деятельности, либо в рамках задач и функций структурных подразделений (должностей), определенных положениями о таких структурных подразделениях (должностными обязанностями). В последнем случае данный порядок должен быть отражен в локальном нормативном акте ОУ, а обработка таких персональных данных должна осуществляться на основании согласия субъекта персональных данных.

Обработка персональных данных без определения правового основания ее необходимости категорически запрещается.

3.8. Перечни идентификаторов персональных данных, используемые для решения задач и функций структурными подразделениями

Для решения тех или иных задач и функций структурными подразделениями ОУ определяются наборы идентификаторов персональных данных, обработка которых вызвана заранее определенной и документированной целью обработки персональных данных.

Обработка персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных недопустима.

Перечни идентификаторов персональных данных, используемые для решения конкретных задач и функций структурными подразделениями в ОУ оформляются в установленном настоящим Положением (пункт 4.5, Приложение 2) порядке.

3.9. Правовое основание обработки персональных данных

3.9.1. Определение законности целей обработки персональных данных

Заявляемые в качестве целей обработки персональных данных цели должны быть законны. Законность целей обработки персональных данных в ОУ определяется наличием любого из указанных оснований:

– наличием федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

– наличие письменного согласия на обработку персональных данных, даваемого субъектом персональных данных;

– наличием договора, одной из сторон которого является субъект персональных данных и в котором оговорены условия обработки персональных данных.

Причем, кроме самого факта обработки персональных данных, должны рассматриваться, и соответственно иметь правовое основание, особые правила обработки определенных наборов

идентификаторов персональных данных (таких как специальные категории персональных данных, биометрические персональные данные и др.), особые способы обработки персональных данных (обработка без использования средств автоматизации, исключительно автоматизированная обработка персональных данных и др.), а так же особые цели обработки персональных данных (однократный пропуск на охраняемую территорию, трансграничная передача персональных данных и др.).

При определении правовых оснований обработки персональных данных должны определяться соответственно:

- статьи и пункты, вид, издавший орган, номер, дата принятия и наименование федерального закона, а также иных подзаконных актов, и документов органов государственной власти, которые требуют обработку персональных данных;
- вид, издавший орган, номер, дата принятия и наименование локального нормативного акта, устанавливающего необходимость получения такого согласия;
- вид, издавший орган, номер, дата принятия и наименование локального нормативного акта, устанавливающего необходимость и форму такого договора

Обработка персональных данных без документально определенного и оформленного правового основания обработки персональных данных не допускается.

3.9.2. Юридические последствия, порождаемые в результате действий (операций) с персональными данными, в отношении субъекта персональных данных либо иным образом затрагивающих права и свободы субъекта персональных данных

К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы.

При обработке персональных данных должны документально определяться и оформляться все возможные юридические последствия в отношении субъекта персональных данных, порождаемые принятием решения на основании использования персональных данных или совершением иных действий с его персональными данными, при выполнении каждой из заявленных задач и функций структурных подразделений (должностных лиц) или видов деятельности учреждения, с учетом особых правил и способов обработки персональных данных.

Определение таких юридических последствий необходимо для недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Обработка персональных данных без документально определенных и оформленных юридических последствий в отношении субъекта персональных данных, порождаемых принятием решения на основании использования персональных данных или совершением иных действий с его персональными данными при выполнении каждой из заявленных задач и функций структурных подразделений (должностных лиц) или видов деятельности учреждения не допускается.

3.9.3. Заданные характеристики безопасности персональных данных

Всеми лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.

Конфиденциальность персональных данных это обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать действий, направленных на передачу персональных данных определенному кругу лиц или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом, без согласия субъекта персональных данных или наличия иного законного основания.

Не требуется обеспечение конфиденциальности:

- в случаях обезличивания персональных данных;
- в отношении общедоступных персональных данных (ставшими таковыми на основании согласия или федерального закона).

При определении заданных характеристик безопасности персональных данных в обязательном порядке должно проверяться наличие законных оснований на присвоение обрабатываемым

персональным данным (для определенных целей обработки) статуса общедоступных персональных данных.

Вне зависимости от необходимости обеспечения конфиденциальности персональных данных, при обработке персональных данных должно определяться наличие требований по обеспечению иных характеристик безопасности персональных данных, отличных от нее.

К таким характеристикам относятся:

- требование по обеспечению защищенности от уничтожения персональных данных;
- требование по обеспечению защищенности от изменения персональных данных;
- требование по обеспечению защищенности от блокирования персональных данных;
- требование по обеспечению защищенности от иных несанкционированных действий.

Обеспечение указанных характеристик безопасности персональных данных может устанавливаться:

- федеральным законом, а также иным подзаконным актом, документом органов государственной власти;
- оператором (ОУ).

При определении необходимости обеспечения характеристик безопасности персональных данных, отличных от конфиденциальности, оператором (ОУ), основным критерием должно служить возникновение юридических последствий для субъекта персональных данных, с чьими персональными данными произошло нарушение таких характеристик безопасности персональных данных.

При принятии решения оператором (ОУ) на обеспечение характеристик безопасности персональных данных, отличных от конфиденциальности, оно должно быть документально определено и оформлено.

Таким образом, при определении характеристик безопасности персональных данных должны определяться:

- законные основания на объявление персональных данных общедоступными;
- статьи и пункты, вид, издавший орган, номер, дата принятия и наименование федерального закона, а также иных подзаконных актов и документов органов государственной власти, которые требуют обеспечения характеристик безопасности, отличных от конфиденциальности;
- вид, издавший орган, номер, дата принятия и наименование локального нормативного акта, устанавливающего требование по обеспечению характеристик безопасности, отличных от конфиденциальности.

Обработка персональных данных без документально определенного и оформленного решения по определению характеристик безопасности персональных данных не допускается.

3.9.4. Определение сроков обработки, в том числе хранения персональных данных

На основании определенных целей обработки персональных данных, способов обработки и образующихся в процессе такой обработки различных видов документов устанавливаются сроки такой обработки, в том числе хранения.

Указанные сроки должны быть документально определены и оформлены в порядке, определяемом настоящим Положением (пункт 4.5, Приложение 2).

Определение сроков хранения осуществляется в соответствии с требованиями архивного законодательства Российской Федерации, в том числе, в соответствии с перечнями типовых архивных документов с указанием сроков их хранения.

При использовании документов, содержащих персональные данные, в различных целях, определение сроков обработки, в том числе хранения, таких документов устанавливается по максимальному сроку. При этом в случае наличия идентификаторов персональных данных в таких документах, обработка которых более не требуется, производятся действия по уничтожению таких данных в порядке, определяемым настоящим Положением (пункт 3.10.7).

Включение в состав Архивного фонда Российской Федерации документов, содержащих персональные данные, осуществляется на основании экспертизы ценности документов и оформляется договором между ОУ и государственным или муниципальным архивом. При этом объем передаваемых документов и условия передачи определяется условиями такого договора и действующими требованиями архивного законодательства Российской Федерации.

На документы, включенные в состав Архивного фонда Российской Федерации, действие настоящего Положения не распространяется.

Обработка персональных данных без документально определенных и оформленных сроков обработки, в том числе хранения персональных данных не допускается.

3.9.5. Контроль за соблюдением сроков обработки персональных данных и фактов достижения целей обработки персональных данных

В ОУ создается комиссия, определяющая факт достижения целей обработки персональных данных и достижение предельных сроков хранения документов, содержащих персональные данные. Порядок работы данной комиссии устанавливается отдельным положением. Правила, устанавливаемые таким положением, не должны противоречить настоящему Положению.

3.10. Действия (операции) с персональными данными;

Обработка персональных данных включает в себя следующие действия (операции) с ними:

1. сбор персональных данных;
2. систематизация персональных данных;
3. накопление персональных данных;
4. распространение персональных данных:
 - 4.1. передача персональных данных определенному кругу лиц (передача персональных данных);
 - 4.2. ознакомление с персональными данными неограниченного круга лиц;
 - 4.3. обнародование персональных данных в средствах массовой информации;
 - 4.4. размещение в информационно-телекоммуникационных сетях;
 - 4.5. предоставление доступа к персональным данным каким-либо иным способом;
5. хранение персональных данных;
6. уточнение персональных данных:
 - 6.1. обновление персональных данных;
 - 6.2. изменение персональных данных;
7. использование персональных данных;
8. обезличивание персональных данных;
9. уничтожение персональных данных;
10. блокирование персональных данных:
 - 10.1. временное прекращение сбор персональных данных а;
 - 10.2. временное прекращение систематизации персональных данных;
 - 10.3. временное прекращение накопления персональных данных;
 - 10.4. временное прекращение использования персональных данных;
 - 10.5. временное прекращение распространения персональных данных;
 - 10.6. временное прекращение передачи персональных данных;
11. снятие блокирования.

Использование иных, отличных от указанных наименований действия (операции) в рамках обработки персональных данных не допускается.

Указанные действия (операции) должны быть документально определены и оформлены в порядке, определяемом настоящим Положением (пункт 4.5, Приложение 2).

Обработка персональных данных без документально определенных и оформленных действий (операций) совершаемых с персональными данными не допускается.

3.10.1. Способы сбора персональных данных и источники их получения

В ОУ приняты следующие способы получения персональных данных субъектов персональных данных:

- заполнение субъектом персональных данных, его законным представителем в случае недееспособности субъекта персональных данных, наследниками в случае смерти субъекта персональных данных или работником ОУ (со слов указанных лиц или путем ввода данных с предъявленных ими документов) соответствующих форм (в том числе для заключения договора), которые утверждаются принятым в ОУ порядке;
- получение персональных данных от третьих лиц на основании письменного согласия субъекта персональных данных (его законного представителя в случае недееспособности субъекта персональных данных или наследников в случае смерти субъекта персональных данных), сбор персональных данных которого производится;
- получение данных на основании запроса третьим лицам в соответствии с действующим

законодательством Российской Федерации, в том числе в ходе досудебных или судебных процессов, с санкции судебных органов выданной в соответствии с действующим законодательством Российской Федерации;

– сбор данных из общедоступных источников.

Получение персональных данных в ОУ допускается только:

- непосредственно от субъекта персональных данных;
- от законного представителя субъекта персональных данных в случае недееспособности субъекта персональных данных;
- от наследников в случае смерти субъекта персональных данных;
- из общедоступных источников;
- от третьих лиц (организаций) в ходе досудебных или судебных процессов, с санкции судебных органов, в соответствии с действующим законодательством Российской Федерации;
- от третьих лиц (организаций), в случаях, установленных действующим законодательством Российской Федерации.

Получение персональных данных из иных источников не допускается.

Законные представители субъекта персональных данных или его наследники обязаны предоставить документы, подтверждающие их полномочия.

В связи с необходимостью постоянного контроля за наличием персональных данных в общедоступных источниках персональных данных, получение и использование таких данных является не рекомендуемым и должно осуществляться только в исключительных случаях в сроки, не превышающие необходимых для принятия соответствующего решения.

3.10.1.1. Правила сбора персональных данных

Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе, за исключением случаев, когда федеральными законами предусматривается обязательное предоставление субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

В случаях, когда федеральными законами не устанавливается обязательность предоставления своих персональных данных, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

Обработка таких персональных данных в ОУ без согласия субъекта персональных данных в письменной форме категорически запрещается.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

При сборе персональных данных субъектов персональных данных на основании согласия или же из общедоступных источников в обязательном порядке необходимо получение согласия в письменной форме, либо указание источника получения общедоступных персональных данных. Обработка в таких случаях без получения письменного согласия субъекта персональных данных или указания общедоступного источника не допускается.

В случаях, когда обязанность предоставления персональных данных установлена федеральным законом, сотрудники ОУ, осуществляющие сбор таких персональных данных, обязаны разъяснить субъекту персональных данных юридические последствия отказа в предоставлении своих персональных данных.

3.10.1.2. Особенности получения персональных данных от третьих лиц

Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены ОУ на основании федерального закона или если персональные данные являются общедоступными, сотрудники ОУ, производившие прием этих данных, перед началом их обработки, обязаны уведомить такого субъекта персональных данных установленным настоящим Положением (пункт 3.14.2) способом.

3.10.2. Способы и правила систематизации, накопления, уточнения и использования персональных данных.

Систематизация, накопление, уточнение, использование персональных данных могут осуществляться любыми законными способами в соответствии с правилами, инструкциями, руководствами,

регламентами и иными документами, определяющими технологический процесс обработки информации.

При систематизации и накоплении персональных данных могут быть установлены особенности учета персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных конкретному субъекту персональных данных.

Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных конкретному субъекту персональных данных.

Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных конкретному субъекту персональных данных.

Уточнение персональных данных должно производиться только на основании законно полученной в установленном порядке информации.

Использование персональных данных должно осуществляться исключительно в заявленных целях. Использование персональных данных в заранее не определенных и не оформленных установленным образом целях категорически не допускается. За нарушение установленных правил обработки персональных данных сотрудники ОУ несут все виды ответственности, предусмотренные действующим законодательством Российской Федерации.

3.10.3. Способы обозначения документов содержащих персональные данные

С целью доведения до сотрудников ОУ фактов работы с документами, содержащими персональные данные, все такие документы (в том числе машинные носители) подлежат специальному обозначению (маркированию, визуальному выделению).

На документах (в том числе на машинных носителях) в правом верхнем углу проставляется:

- в первой строке: Содержит персональные данные;
- во второй строке: полное наименование ОУ.

В третьей строке, при необходимости, дополнительно могут проставляться иные реквизиты документа, в том числе его регистрационный номер по журналам учета.

Ответственным за специальное обозначение документов является их исполнитель.

Специальное обозначение осуществляется при печати документов машинным способом или путем проставления штампа на ранее созданных документах и машинных носителях (в свободном месте на имеющихся наклейках или на специально наклеенном листе или корпусе носителя).

Специальное обозначение ранее созданных документов должно производиться при обращении к ним.

3.10.4. Способы передачи персональных данных и их получатели

В ОУ приняты следующие способы передачи персональных данных субъектов персональных данных:

- передача персональных данных на электронных носителях информации посредством нарочного;
- передача персональных данных на бумажных носителях посредством нарочного;
- передача персональных данных на электронных носителях посредством почтовой связи;
- передача персональных данных на бумажных носителях посредством почтовой связи;
- передача персональных данных по каналам электрической связи;
- трансграничная передача персональных данных по каналам электрической связи.

Передача персональных данных из ОУ допускается только:

- непосредственно субъекту персональных данных (его законному представителю в случае недееспособности субъекта персональных данных или наследникам в случае смерти субъекта персональных данных) на основании запроса, если предоставление персональных данных не нарушает конституционные права и свободы других лиц;
- третьим лицам на основании письменного согласия (в целях исполнения договора, одной из сторон которого является субъект персональных данных и в котором оговорены назначение и условия такой передачи) субъекта персональных данных (его законного представителя в случае недееспособности субъекта персональных данных или наследников в случае смерти субъекта персональных данных), сбор персональных данных которого производится;
- на основании официального запроса от третьих лиц (организаций) в ходе досудебных или судебных процессов, с санкции судебных органов, в соответствии с действующим законодательством Российской Федерации;

– на основании официального запроса от третьих лиц (организаций), если обязанность по передаче таких персональных данных установлена действующим законодательством Российской Федерации.

Законные представители субъекта персональных данных или его наследники обязаны предоставить документы, подтверждающие их полномочия.

3.10.4.1. Особенности передачи персональных данных третьим лицам

При передаче персональных данных, за исключением передачи персональных данных субъекту персональных данных (его законному представителю в случае недееспособности субъекта персональных данных или наследникам в случае смерти субъекта персональных данных), лица, получающие персональные данные, должны быть предупреждены о:

- факте обработки ими персональных данных;
- категориях обрабатываемых персональных данных;
- том, что эти данные могут быть использованы лишь в целях, для которых они сообщены;
- необходимости соблюдения конфиденциальности таких персональных данных;
- 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 учреждения ОУ.

Законные представители субъекта персональных данных или его наследники обязаны предоставить документы, подтверждающие их полномочия.

Получатели персональных данных обязаны подтвердить соблюдение этих правил.

3.10.4.2. Особенности передачи персональных данных субъектам персональных данных, их законным представителям и наследникам

Передача персональных данных субъектам персональных данных, их законным представителям и наследникам осуществляется на основании официального запроса или обращения.

Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных, его законного представителя или наследника;
- сведения о дате, месте выдачи указанного документа и выдавшем его органе;
- собственноручную подпись субъекта персональных данных, его законного представителя или наследника.

В случае получения запроса от законного представителя или наследника субъекта персональных данных к такому запросу должны прилагаться документы, подтверждающие полномочия указанных лиц в соответствии с действующим законодательством Российской Федерации.

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных, его законному представителю или наследнику в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Доступность формы определяется самим запросом и может быть ограничена принятым в ОУ в соответствии с действующим законодательством Российской Федерации режимом ограничения доступа к информации.

3.10.5. Хранение персональных данных

Хранение персональных данных в ОУ допускается только в форме документов – зафиксированной на материальном носителе информации (содержащей персональные данные) с реквизитами, позволяющими ее идентифицировать и определить субъекта персональных данных. При этом предусматриваются следующие виды документов:

- изобразительный документ – документ, содержащий информацию, выраженную посредством изображения какого-либо объекта
- фотодокумент – изобразительный документ, созданный фотографическим способом;
- текстовый документ – документ, содержащий речевую информацию, зафиксированную любым типом письма или любой системой звукозаписи;
- письменный документ – текстовый документ, информация которого зафиксирована любым типом письма;
- рукописный документ – письменный документ, при создании которого знаки письма наносят от руки;

- машинописный документ – письменный документ, при создании которого знаки письма наносят техническими средствами;
- документ на машинном носителе – документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

3.10.6. Способы и порядок блокирования персональных данных

В случаях, предусмотренных настоящим Положением, осуществляется блокирование персональных данных. При этом до снятия блокировки категорически запрещается сбор, систематизация, накопление, использование, распространение персональных данных о субъекте персональных данных, чьи персональные данные блокированы, в том числе их передача.

3.10.7. Способы и порядок уничтожения персональных данных

Уничтожение персональных данных это действия, в результате которых невозможно восстановить содержание персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Уничтожение персональных данных в ОУ производится только в следующих случаях:

- по достижении целей обработки или в случае утраты необходимости в их достижении;
- по требованию субъекта персональных данных в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- при выявлении неправомерных действий с персональными данными и невозможности устранения допущенных нарушений;
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;
- по требованию уполномоченного органа по защите прав субъектов персональных данных в случае недостоверных или полученных незаконным путем персональных данных.

По факту уничтожения персональных данных обязательно проверяется необходимость уведомления об этом и в случае наличия такого требования, осуществляется уведомление указанных в таком требовании лиц, в порядке, приведенном в настоящем Положении.

При уничтожении персональных данных необходимо:

- убедиться в необходимости уничтожения персональных данных;
- убедиться в том, что уничтожаются те персональные данные, которые предназначены для уничтожения;
- уничтожить персональные данные подходящим способом, в соответствии с настоящим Положением или способом, указанным в соответствующем требовании или распорядительном документе;
- проверить необходимость уведомления об уничтожении персональных данных;
- при необходимости, уведомить об уничтожении персональных данных требуемых лиц.

При уничтожении персональных данных применяются следующие способы:

- измельчение в бумагорезательной (бумагоуничтожительной) машине – для документов исполненных на бумаге;
- тщательное вымарывание (с проверкой тщательности вымарывания) – для сохранения возможности обработки иных данных, зафиксированных на материальном носителе, содержащем персональные данные;
- измельчение в специальной бумагорезательной (бумагоуничтожительной) машине или физическое уничтожение (разрушение) носителей информации – для носителей информации на оптических дисках;
- физическое уничтожение частей носителей информации – разрушение или сильная деформация – для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы), USB- и Flash-носителях (уничтожению подлежат модули и микросхемы долговременной памяти);
- стирание с помощью сертифицированных средств уничтожения информации – для записей в базах данных и отдельных документов на машинном носителе.

При уничтожении персональных данных необходимо учитывать их наличие в архивных базах данных и производить уничтожение во всех копиях базы данных, если иное не установлено

действующим законодательством Российской Федерации.

При необходимости уничтожения части персональных данных допускается уничтожать материальный носитель одним из указанных в настоящем Положении способов, с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

Уничтожение персональных данных производится ответственными за носители персональных данных только в присутствии Руководителя ОУ или его заместителей.

По факту уничтожения персональных данных составляется Акт уничтожения персональных данных, по форме, приведенной в Приложении 8, который подписывается лицами, производившими уничтожение, заверяется заместителем Руководителя ОУ, присутствовавшим при уничтожении и утверждается Руководителем ОУ.

Хранение актов уничтожения персональных данных осуществляется в течении срока исковой давности, если иное не установлено нормативно-правовыми актами Российской Федерации.

3.11. Круг субъектов, персональные данные которых подлежат обработке

Круг субъектов, персональные данные которых подлежат обработке, определяется целью обработки персональных данных в каждой из заявленных функций и задач структурных подразделений (должностных обязанностей) и соответствующим видом деятельности ОУ.

3.12. Перечень должностных лиц, осуществляющих обработку персональных данных

Заместитель Руководителя ОУ ежегодно готовит перечень должностных лиц, осуществляющих обработку персональных данных, в котором указываются:

- должность должностного лица, допущенного к обработке персональных данных, в соответствии со штатным расписанием ОУ;
- фамилия, имя, отчество;
- полномочия для доступа к информации (персональным данным).

Перечень подписывается заместителем Руководителя ОУ и утверждается Руководителем ОУ.

В случае необходимости внесения изменений в указанный перечень, составляется дополнение к нему. Дополнение согласовывается и утверждается в установленном для перечня порядке.

3.13. Права и обязанности при обработке персональных данных

3.13.1. Права и обязанности субъекта персональных данных

3.13.1.1. Права субъекта персональных данных

Субъект персональных данных, чьи персональные данные обрабатываются в ОУ, имеет право:

- давать своей волей и в своем интересе и отзывать согласие на обработку своих персональных данных в предусмотренных действующим законодательством Российской Федерации случаях;
- требовать от ОУ разъяснения порядка принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения;
- требовать разъяснения юридических последствий отказа предоставить свои персональные данные, если обязанность предоставления персональных данных установлена федеральным законом;
- заявить возражение против исключительно автоматизированной обработки его персональных данных;
- на получение в доступной форме сведений об ОУ (в объеме необходимом для защиты своих прав и законных интересов по вопросам обработки своих персональных данных), о месте нахождения ОУ, о наличии у ОУ своих персональных данных;
- подавать запрос на доступ к своим персональным данным;
- получить в письменной форме мотивированный ответ с указанием федерального закона, являющегося основанием для отказа в предоставлении субъекту персональных данных при обращении либо при получении запроса субъекта персональных данных информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных;
- требовать безвозмездного предоставления возможности ознакомления с его персональными данными;

- требовать от ОУ уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- получать уведомления по вопросам обработки его персональных данных в установленных действующим законодательством Российской Федерации случаях и сроки;
- требовать от ОУ разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов;
- обжаловать действия или бездействие ОУ в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

При требовании субъектом персональных данных предоставления сведений о работниках ОУ, задействованных в обработке его персональных данных, предоставляются данные о наименовании структурных подразделений и должностей таких сотрудников.

Кроме указанных прав в вопросах обработки его персональных данных субъект персональных данных обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

3.13.1.2. Обязанности субъекта персональных данных

Субъект персональных данных, чьи персональные данные обрабатываются в ОУ, обязан:

- предоставлять свои персональные данные в случаях, когда федеральными законами предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;
- с целью соблюдения его законных прав и интересов подавать только достоверные персональные данные.

Кроме указанных обязанностей в вопросах обработки его персональных данных на субъекта персональных данных налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации.

3.13.2. Права и обязанности ОУ при обработке персональных данных субъектов персональных данных

3.13.2.1. Права ОУ при обработке персональных данных субъектов персональных данных

ОУ при обработке персональных данных субъектов персональных данных имеет право:

- обрабатывать персональные данные субъектов персональных данных без получения согласия субъекта персональных данных в предусмотренных действующим законодательством целях, объемах и случаях;
- письменно мотивированно отказать субъекту персональных данных в получении информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных, в случаях предусмотренных действующим законодательством Российской Федерации, в том числе, если обработка персональных данных осуществляется в целях охраны правопорядка или предоставление персональных данных нарушает конституционные права и свободы других лиц.

Кроме указанных прав в вопросах обработки персональных данных субъектов персональных данных ОУ обладает другими правами, предоставляемыми ему действующим законодательством Российской Федерации.

3.13.2.2. Обязанности ОУ при обработке персональных данных субъектов персональных данных

ОУ при обработке персональных данных субъектов персональных данных обязано:

- неукоснительно соблюдать принципы обработки персональных данных отраженные в настоящем Положении;
- неукоснительно соблюдать все требования настоящего Положения;
- предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки общедоступных персональных данных

обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными;

– проинформировать лиц (включая сотрудников ОУ или лиц, осуществляющих такую обработку по договору с ОУ), осуществляющих обработку персональных данных, в том числе без использования средств автоматизации, о факте обработки ими персональных данных, 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 ОУ.

Кроме указанных обязанностей в вопросах обработки персональных данных субъектов персональных данных на ОУ налагаются иные обязанности, предусмотренные действующим законодательством Российской Федерации, в том числе законодательством об образовательной деятельности.

3.14. Порядок взаимодействия с субъектами персональных данных

3.14.1. Установленные сроки выполнения действий по защите прав субъектов персональных данных

В ОУ устанавливаются следующие сроки по защите прав субъектов персональных данных:

– обработка специальных категорий персональных данных должна быть прекращена **незамедлительно**, если устранены причины, вследствие которых осуществлялась;

– ОУ обязано рассмотреть возражения на принятие решения на основании исключительно автоматизированной обработки персональных данных субъекта персональных данных в течение **семи рабочих дней со дня его получения** и уведомить субъекта персональных данных о результатах рассмотрения такого возражения;

– ОУ обязано сообщить субъекту персональных данных информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных либо **в течение десяти рабочих дней с даты получения запроса** субъекта персональных данных или его законного представителя;

– в случае отказа в предоставлении субъекту персональных данных при обращении либо при получении запроса субъекта персональных данных информации о наличии его персональных данных, а также таких персональных данных ОУ обязано дать в письменной форме мотивированный ответ, содержащий ссылку на положение федерального закона, являющееся основанием для такого отказа, в срок, не превышающий **семи рабочих дней** со дня обращения субъекта персональных данных либо **с даты получения запроса** субъекта персональных данных;

– в случае выявления недостоверных персональных данных или неправомерных действий с ними в ОУ при обращении или по запросу субъекта персональных данных либо уполномоченного органа по защите прав субъектов персональных данных ОУ обязано осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, **с момента такого обращения или получения такого запроса на период проверки**;

– ОУ обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, **в течение семи рабочих дней с даты получения такого запроса**;

– в случае выявления неправомерных действий с персональными данными ОУ в срок, не превышающий **трех рабочих дней с даты такого выявления**, обязано устранить допущенные нарушения;

– в случае невозможности устранения допущенных нарушений ОУ в срок, не превышающий **трех рабочих дней с даты выявления неправомерности действий** с персональными данными, обязано уничтожить персональные данные;

– в случае достижения цели обработки персональных данных ОУ обязано незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий **трех рабочих дней с даты достижения цели** обработки персональных данных, если иное не предусмотрено федеральными законами;

– в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных ОУ обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий **трех рабочих дней с даты поступления**

указанного отзыва, если иное не предусмотрено соглашением между ОУ и субъектом персональных данных.

Установленные сроки обязательны к исполнению всеми должностными лицами ОУ.

3.14.2. Требования по уведомлениям субъектов персональных данных и в иных случаях

Подача уведомлений осуществляется в следующих случаях:

- ОУ обязано уведомить субъекта персональных данных по результатам рассмотрения возражения о принятии решения при обработке персональных данных субъекта персональных данных на основании исключительно автоматизированной обработки его персональных данных;
- ОУ обязано уведомить субъекта персональных данных и третьих лиц, которым персональные данные этого субъекта были переданы, о внесенных изменениях и предпринятых мерах по уничтожению или блокированию соответствующих персональных данных на основании предоставленных субъектом персональных данных сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет ОУ являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- об устранении выявленных неправомерных действий с персональными данными или об уничтожении персональных данных, в случае невозможности устранения допущенных нарушений, ОУ обязано уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган;
- ОУ обязано уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган, о прекращении обработки персональных данных и уничтожении соответствующих персональных данных в случае достижения цели обработки персональных данных;
- ОУ обязано уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган, о прекращении обработки персональных данных и уничтожении соответствующих персональных данных в случае отзыва субъектом персональных данных согласия на обработку своих персональных;
- ОУ обязано уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных в установленных действующим законодательством случаях, а так же об изменениях поданных сведений;
- если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены на основании федерального закона или если персональные данные являются общедоступными, ОУ до начала обработки таких персональных данных обязано предоставить субъекту персональных данных следующую информацию: наименование и адрес ОУ или ее представителя, цель обработки персональных данных и ее правовое основание, предполагаемые пользователи персональных данных, установленные действующим законодательством РФ в области персональных данных права субъекта персональных данных.

Уведомление в указанных случаях готовиться заместителем Руководителя ОУ. Подготовленное уведомление утверждается Руководителем ОУ. Отправка уведомления осуществляется заместителем Руководителя ОУ в установленные настоящим Положением (пункт 3.14.1) сроки.

Форма уведомлений о совершенных операциях над персональными данными приведена в Приложении 9.

Требования к уведомлению уполномоченного органа по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных и об изменении поданных сведений устанавливаются настоящим Положением (пункт 3.16).

3.14.3. Порядок разъяснения субъектам персональных данных особенностей обработки персональных данных и порядка защиты их прав

Сотрудники ОУ обязаны разъяснять субъектам персональных данных особенности обработки персональных данных и порядок защиты их прав в следующих случаях:

- при принятии решения на основании исключительно автоматизированной обработки его

персональных данных – разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных, возможные юридические последствия такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов;

– если обязанность предоставления персональных данных установлена федеральным законом – разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

Разъяснения осуществляются на основании настоящего Положения, Юридических паспортов ИСПДн и действующего законодательства Российской Федерации в области персональных данных.

3.14.4. Порядок реагирования на обращения субъектов персональных данных

Все обращения субъектов персональных данных принимаются в письменном виде и подлежат учету, наряду с остальными входящими документами.

С целью соблюдения сроков по реагированию на обращения субъектов персональных данных они должны незамедлительно передаваться Руководителю ОУ.

Ответы на обращения, не отвечающие требованиям, предъявляемым к ним действующим законодательством в области персональных данных, не производятся.

Передача ответов субъекту персональных данных осуществляется требуемым им способом, или, если такой способ не указан, посредством отправки заказного письма с уведомлением.

Передача ответов на обращения субъектов персональных данных осуществляется по журналам исходящих документов в установленные настоящим Положением (пункт 3.14.1) сроки с указанием в таких журналах способа передачи ответа, а также отметки о доставке с указанием реквизитов уведомления о доставке, если такой ответ направлялся посредством почтовой связи.

3.14.5. Порядок действий при обращениях субъектов персональных данных

3.14.5.1. Требования к форме запроса на предоставления персональных данных и сведений об операторе субъектом персональных данных

Доступ к своим персональным данным предоставляется субъекту персональных данных при обращении либо при получении запроса субъекта персональных данных. Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- собственноручную подпись субъекта персональных данных.

Запросы, не отвечающие указанным требованиям, не подлежат обработке.

3.14.5.2. Порядок и основание отказа субъекту персональных данных в предоставлении сведений о его персональных данных

Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если предоставление персональных данных нарушает конституционные права и свободы других лиц.

В случае отказа в предоставлении субъекту персональных данных при обращении, либо при получении запроса субъекта персональных данных информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных, заместитель Руководителя ОУ составляет в письменной форме мотивированный ответ, содержащий ссылку на пункты или статьи федерального закона, являющегося основанием для такого отказа.

3.14.5.3. Порядок, форма предоставления персональных данных и сведений об операторе и объем предоставляемой информации

Предоставление доступа к своим персональным данным в случае непосредственного обращения субъекта персональных данных осуществляется только по адресу: 644099, г. Омск, наб. Тухачевского, 14, федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Омский государственный педагогический университет». Доступ субъекта персональных данных в этом случае осуществляется по предъявлению основного документа, удостоверяющего личность субъекта персональных данных с обязательным

составлением запроса, отвечающего требованиям настоящего Положения.

Субъект персональных данных имеет право на получение при обращении или при подаче запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором, а также цель такой обработки;
- способы обработки персональных данных, применяемые оператором;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Ответ на обращения субъектов персональных данных готовится заместителем Руководителя ОУ по существу такого обращения в двух экземплярах. Запрашиваемые сведения предоставляются в соответствии с Юридическим паспортом ИСПДн и настоящим Положением.

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Форму предоставления данных определяет заместитель Руководителя ОУ, если она не оговорена в таком обращении. Форма ответа на обращение субъекта персональных данных не должна противоречить установленным в ОУ требованиям по защите информации и обеспечению безопасности персональных данных.

Хранение обращения субъекта персональных данных, а так же второй экземпляр ответа на такое обращение, хранятся установленным в ОУ порядке.

3.14.5.4. Действия в случае выявления фактов нарушения законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных

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

В случае выявления недостоверных персональных данных или неправомерных действий с ними ОУ при обращении или по запросу субъекта персональных данных либо уполномоченного органа по защите прав субъектов персональных данных осуществляется блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

В случае подтверждения факта недостоверности персональных данных ОУ на основании документов, представленных субъектом персональных данных либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано снять с персональных данных блокирование и уточнить их.

В случае выявления неправомерных действий с персональными данными ОУ обязано устранить допущенные нарушения.

В случае невозможности устранения допущенных нарушений ОУ обязано уничтожить (пункт 3.10.7) персональные данные.

При этом должны соблюдаться определенные настоящим Положением (пункт 3.14.1) сроки и требования по уведомлению о совершенных действиях.

При обнаружении нарушений правил обработки или обеспечения безопасности персональных данных лица ответственные за такую обработку в ОУ незамедлительно принимают меры по устранению таких нарушений и минимизации их последствий. При этом должен проводиться анализ этих нарушений и приниматься меры по недопущению таких нарушений в дальнейшем.

В случае если произошло нарушение прав субъекта персональных данных и данное нарушение может повлиять на поражение прав такого субъекта в дальнейшем, ОУ организует оповещение этого субъекта о возможных последствиях выявленных нарушений и принятых по ним мерах. Порядок такого оповещения устанавливается в каждой конкретной ситуации ответственными за такое оповещение

лицами.

3.14.5.5. Право на обжалование действий или бездействия оператора

Если субъект персональных данных считает, что ОУ осуществляет обработку его персональных данных с нарушением требований законодательства в области персональных данных или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие ОУ в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

3.14.6. Порядок действий при достижении целей обработки персональных данных и отзыве согласия на обработку персональных данных

В случае достижения целей обработки персональных данных ОУ обязано незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные, если иное не предусмотрено федеральными законами.

В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных ОУ обязано прекратить обработку персональных данных и уничтожить персональные данные, если иное не предусмотрено соглашением между ОУ и субъектом персональных данных.

При этом должны соблюдаться определенные настоящим Положением (пункт 3.14.1) сроки и требования по уведомлению о совершенных действиях.

3.14.7. Порядок действий при отзыве согласия субъекта персональных данных на обработку его персональных данных

Заявление на отзыв согласия на обработку персональных данных подается в письменном виде лицом, указанным в согласии на обработку персональных данных, лично. Заявление на отзыв согласия на обработку персональных данных должно содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- собственноручную подпись субъекта персональных данных;
- сведения о согласии на обработку персональных данных (дата и адрес, по которому давалось согласие).

При подаче заявления, лицом, осуществляющим прием такого заявления, производится удостоверение личности подающего такое заявление.

Подача заявления осуществляется по адресу регистрации юридического лица (его правопреемника), которому давалось согласие на обработку персональных данных.

В случае недееспособности субъекта персональных данных заявление на отзыв согласия на обработку персональных данных подает законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных заявление на отзыв согласия на обработку персональных данных подают наследники субъекта персональных данных, если такое заявление не было подано субъектом персональных данных при его жизни.

В случае подачи заявления на отзыв согласия на обработку персональных данных от законного представителя субъекта персональных данных или наследников субъекта персональных данных, они обязаны предоставить документы, подтверждающие их полномочия.

3.15. Согласие субъекта персональных данных на обработку его персональных данных

Настоящим Положением устанавливаются требования к содержанию письменного согласия субъекта персональных данных на обработку его персональных данных и его форма. Равнозначным содержащему собственноручную подпись письменному согласию субъекта персональных данных на бумажном носителе признается согласие в форме электронного документа, подписанного электронной цифровой подписью или в случаях, предусмотренных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами, иным аналогом собственноручной подписи.

Использование иных форм согласия, отличных от указанных, не допускается.

Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие;
- порядок защиты субъектом персональных данных своих прав и законных интересов;
- порядок отзыва согласия;
- собственноручную подпись субъекта персональных данных.

В случае если обязанность предоставления персональных данных установлена федеральным законом в согласие должны включаться:

- юридические последствия отказа предоставить свои персональные данные, если обязанность предоставления персональных данных установлена федеральным законом.

В случае исключительно автоматизированной обработки персональных данных в согласие должны включаться:

- порядок принятия решения на основании исключительно автоматизированной обработки персональных данных субъекта персональных данных;
- возможные юридические последствия решения на основании исключительно автоматизированной обработки персональных данных субъекта персональных данных;
- возможность заявить возражение против решения исключительно автоматизированной обработки своих персональных данных;
- разъяснения о порядке защиты субъектом персональных данных своих прав и законных интересов.

В случае обработки персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи в согласие должны включаться:

- цель обработки: «продвижение товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи».

В случае обработки специальных категорий персональных данных в согласие должны включаться:

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных: «сведения о состоянии здоровья работника ОУ в объеме сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции» или «сведения о состоянии здоровья учащегося ОУ в объеме сведений, которые относятся к вопросу об оказании ему образовательных услуг, а также охраны его здоровья».

В случае обработки биометрических персональных данных в согласие должны включаться:

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных: «личная подпись», «фотография» и др.

В случае передачи персональных данных третьим лицам в согласие должны включаться:

- наименование и адрес оператора, которому будут передаваться персональные данные;
- цель передачи персональных данных;
- перечень персональных данных, на передачу которых дается согласие субъекта персональных данных;
- срок, в течение которого действует согласие на передачу;
- собственноручную подпись субъекта персональных данных.

В случае договорных отношений, включающих обработку персональных данных, такие договоры должны содержать все положения, указываемые в согласии на обработку персональных данных субъекта персональных данных.

Для обработки персональных данных, содержащихся в согласии в письменной форме субъекта на обработку его персональных данных, дополнительного согласия не требуется.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта персональных

данных, в случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни. В указанных случаях к согласию на обработку персональных данных прилагаются документы (копии), подтверждающие полномочия указанных лиц.

В согласие вносятся сведения, определяемые юридическим паспортом информационной системы персональных данных и настоящим Положением (пункт 3.15).

3.16. Уведомление об обработке (о намерении осуществлять обработку) персональных данных

ОУ уведомляет уполномоченный орган по защите прав субъектов персональных данных об осуществлении обработки персональных данных, а также в случае изменения представленных в уведомлении сведений.

При этом должны соблюдаться установленные настоящим Положением (3.14.1) сроки подачи уведомлений.

ОУ вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

- относящихся к субъектам персональных данных, которых связывают с ОУ трудовые отношения;
- полученных ОУ в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- являющихся общедоступными персональными данными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится ОУ, или в иных аналогичных целях;
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Уведомление об обработке персональных данных должно быть направлено в письменной форме и подписано Руководителем ОУ.

Уведомление должно содержать следующие сведения:

- наименование ОУ;
- адрес ОУ;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных.

Форма уведомления об обработке персональных данных устанавливается нормативным актом федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере информационных технологий и связи.

В случае предоставления неполных или недостоверных сведений, уполномоченный орган по защите прав субъектов персональных данных вправе требовать уточнения предоставленных сведений до их внесения в реестр операторов.

Уведомление об обработке персональных данных готовится заместителем Руководителя ОУ. Изменения в уведомление готовит структурное подразделение, являющееся инициатором изменений в обработке персональных данных. Изменения согласовываются с заместителем Руководителя ОУ. Отсылку изменений производит заместитель Руководителя ОУ.

4. Организация обработки персональных данных в ОУ

4.1. Организационная структура и функции ОУ

Организационная структура ОУ определяется в соответствии со Штатным расписанием (форма Т-3), утвержденным Руководителем ОУ.

Виды деятельности ОУ определяются Уставом федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Омский государственный педагогический университет», утвержденным Министерством образования и науки Российской Федерации.

Функции ОУ, связанные с обработкой персональных данных, реализуются только в соответствии с заявленными видами деятельности, а также в соответствии с действующим трудовым, бухгалтерским, налоговым и иными видами законодательства Российской Федерации, определяющими внутреннюю деятельность учреждения.

4.2. Задачи и функции подразделений

В каждом подразделении ОУ разрабатываются положения, утверждаемые Руководителем ОУ, конкретизирующие операции по заявленным в Уставе ОУ видам деятельности. Все операции соответствуют действующему законодательству Российской Федерации и разрабатываются на основе федеральных законов, нормативных документов органов государственной власти Российской Федерации.

4.3. Направления обработки персональных данных в ОУ

Обработка персональных данных в ОУ осуществляется по следующим направлениям:

- в рамках деятельности ОУ как образовательного учреждения, в соответствии с Федеральным Законом РФ №3266-1 от 10 июля 1992 г. «Об образовании»;
- в рамках деятельности ОУ в качестве работодателя;
- в рамках деятельности ОУ в качестве собственника обособленного имущества.

4.3.1. Обработка персональных данных в рамках деятельности ОУ в качестве образовательного учреждения

При обработке персональных данных в рамках деятельности образовательного учреждения ОУ руководствуется следующими нормативно-правовыми актами и документами:

- Конституцией Российской Федерации, принятой на всенародном голосовании 12.12.1993 г.;
- Федеральным Законом РФ №3266-1 от 10 июля 1992 г. «Об образовании»;
- и другими.

4.3.2. Обработка персональных данных в рамках деятельности ОУ в качестве работодателя

При обработке персональных данных в рамках деятельности учреждения в качестве работодателя ОУ руководствуется следующими нормативно-правовыми актами и документами:

- Федеральным Законом РФ №197-ФЗ от 30.12.2001 г. «Трудовой Кодекс Российской Федерации»;
- Федеральным Законом РФ №129-ФЗ от 21.11.1996 г. «О бухгалтерском учете»;
- Федеральными законами РФ №146-ФЗ от 31.07.1998 г., №117-ФЗ от 05.07.2000 г. «Налоговый Кодекс Российской Федерации»;
- Федеральный закон №27-ФЗ от 01.04.1996 г. «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
- Законом РФ №3266-1 от 10.07.1992 г. «Об образовании»;
- Постановлением Государственного комитета Российской Федерации по статистике №1 от 05.01.2004 г. «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;
- Федеральным законом №255-ФЗ от 29.12.2006 г. «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;
- Федеральным законом №167-ФЗ от 15.12.2001 г. «Об обязательном пенсионном страховании в Российской Федерации»;
- Федеральным законом №212-ФЗ от 24.07.2009 г. «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд

обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования);

- Законом №5487-1 от 22.07.1993 г. «Основы законодательства Российской Федерации об охране здоровья граждан»;
- законодательством РФ по вопросам статистической отчетности;
- и другими.

4.3.3. Обработка персональных данных в рамках деятельности в качестве собственника имущества

При обработке персональных данных в рамках деятельности учреждения в качестве собственника обособленного имущества ОУ руководствуется следующими нормативно-правовыми актами и документами:

- Конституцией Российской Федерации, принятой на всенародном голосовании 12.12.1993 г.;
- Федеральными законами РФ №51-ФЗ от 30.11.1994 г., №14-ФЗ от 26.12.1996 г., №146-ФЗ от 26.11.2001 г., №230-ФЗ от 18.12.2006 г. «Гражданский кодекс Российской Федерации»;
- Федеральным законом РФ №63-ФЗ от 13.06.1996 г. «Уголовный кодекс РФ»;
- Федеральным законом РФ №195-ФЗ от 30.12.2001 г. «Кодекс Российской Федерации об административных правонарушениях»;
- рекомендациями, руководящими документами и стандартами МВД РФ;
- Федеральным законом от 14.04.1999 г. №77-ФЗ «О ведомственной охране»;
- Постановлением Правительства РФ №589 от 14.08.1992 г. «Об утверждении Положения о вневедомственной охране при органах внутренних дел Российской Федерации»;
- Законом РФ №2487-1 от 11.03.1992 г. «О частной детективной и охранной деятельности в Российской Федерации»;
- Законом РФ №1026-1 от 18.04.1991 г. «О милиции»;
- и другими.

4.4. Информационные системы персональных данных

4.4.1. Критерии определения информационных систем персональных данных в ОУ

Все информационные системы ОУ, в которых производится обработка персональных данных, являются информационными системами персональных данных. Информационная система персональных данных состоит из совокупности:

- базы данных, в состав которой входят персональные данные;
- информационных технологий, позволяющих осуществлять обработку, содержащихся в базе данных персональных данных;
- технических средств, позволяющих осуществлять обработку, содержащихся в базе данных персональных данных.

Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без использования таких средств.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Частным случаем автоматизированной обработки персональных данных является исключительно автоматизированная обработка персональных данных, при осуществлении которой решения, порождающие юридические последствия в отношении субъекта персональных данных или иным

образом затрагивающее его права и законные интересы, принимаются на основании исключительно автоматизированной обработки его персональных данных.

Обязательным условием создания информационной системы персональных данных является наличие обособленной базы данных, содержащей персональные данные, при изоляции которой от других информационных систем персональных данных, возможна обработка содержащихся в ней персональных данных с помощью информационных технологий и технических средств, входящих в состав этой информационной системы персональных данных.

Допускается использование одних и тех же информационных технологий и технических средств, для обработки различных баз данных, содержащих персональные данные, при этом разделение на различные информационные системы персональных данных производится по критерию уникальности баз данных, содержащих персональные данные.

4.4.2. Наименование информационной системы персональных данных

С целью идентификации каждой информационной системе персональных данных в ОУ присваивается наименование, которое должно отражать основное назначение данной информационной системы либо наименование программных средств обработки персональных данных в данной информационной системе персональных данных.

4.4.3. Цели создания или эксплуатации информационной системы персональных данных

Для каждой информационной системы персональных данных определяются цели ее создания и эксплуатации. При этом определяется предполагаемое назначение информационной системы персональных данных, в соответствии с предлагаемыми услугами, осуществляемыми информационной системой персональных данных внутренними задачами или с определенными требованиями, предъявляемыми действующим в Российской Федерации законодательством.

4.4.4. Параметры, характеризующие информационную систему персональных данных

Для каждой информационной системы персональных данных определяются следующие параметры, характеризующие такую информационную систему персональных данных:

- цель обработки персональных данных в информационной системе персональных данных;
- способы обработки персональных данных в информационной системе персональных данных;
- перечень сведений, содержащих персональные данные о субъекте персональных данных, обрабатываемых в информационной системе персональных данных;
- необходимость обработки персональных данных в информационной системе персональных данных;
- правовое основание обработки персональных данных в информационной системе персональных данных;
- юридические последствия, порождаемые в результате действий (операций) с персональными данными в информационной системе персональных данных, в отношении субъекта персональных данных либо иным образом затрагивающих права и свободы субъекта персональных данных;
- круг субъектов, персональные данные которых подлежат обработке в информационной системе персональных данных;
- перечень действий (операций) с персональными данными в информационной системе персональных данных;
- заданные характеристики безопасности персональных данных в информационной системе персональных данных;
- перечень должностных лиц структурных подразделений, осуществляющих обработку персональных данных в информационной системе персональных данных;
- юридические последствия отказа в предоставлении персональных данных субъектов персональных данных для их обработки в информационной системе персональных данных;
- места обработки персональных данных в рамках информационной системы персональных данных;
- перечень применяемого в информационной системе персональных данных при обработке персональных данных специального программного обеспечения, средств управления базами данных;

- перечень баз данных и иных массивов информации в информационной системе персональных данных, содержащих персональные данные;
- функциональные и технологические связи как внутри информационной системы персональных данных, так и с другими информационными системами персональных данных;
- способы и источники получения персональных данных;
- способы передачи персональных данных и их получатели;
- сроки обработки, в том числе хранения персональных данных в информационной системе персональных данных.

4.5. Юридический паспорт информационной системы персональных данных

В ОУ вводится понятие Юридического паспорта информационной системы персональных данных (далее – Паспорт ИСПДн). Паспорт ИСПДн разрабатывается на каждую информационную систему персональных данных в ОУ.

Паспорт ИСПДн содержит:

- наименование информационной системы персональных данных;
- цели создания или эксплуатации информационной системы персональных данных;
- цель обработки персональных данных в информационной системе персональных данных;
- способы обработки персональных данных;
- перечень идентификаторов персональных данных о субъекте персональных данных, обрабатываемых в информационной системе персональных данных;
- необходимость и правовое основание обработки персональных данных в информационной системе персональных данных;
- необходимость получения согласия субъекта персональных данных на обработку его персональных данных;
- юридические последствия, порождаемые в результате действий (операций) с персональными данными, в отношении субъекта персональных данных либо иным образом затрагивающих права и свободы субъекта персональных данных;
- круг субъектов, персональные данные которых подлежат обработке в информационной системе персональных данных;
- количество субъектов персональных данных, чьи персональные данные обрабатываются;
- действия (операции) с персональными данными в информационной системе персональных данных;
- способы и источники получения персональных данных;
- способы передачи персональных данных и их получатели;
- определение сроков обработки, в том числе хранения персональных данных в информационной системе персональных данных;
- юридические последствия отказа в предоставлении своих персональных данных;
- заданные характеристики безопасности обрабатываемых в информационной системе персональных данных;
- места обработки персональных данных;
- характеристики средств автоматизации обработки персональных данных;
- функциональные связи информационной системы персональных данных;
- лист ознакомления.

Форма «Паспорта ИСПДн» и порядок его заполнения устанавливается настоящим Положением (Приложение 2).

Паспорт ИСПДн утверждается приказом Руководителя ОУ.

Паспорта ИСПДн хранятся у заместителя Руководителя ОУ.

Паспорт ИСПДн должен отражать все параметры, характеризующие информационную систему персональных данных.

Все поля Паспорта ИСПДн должны быть заполнены, не заполнение полей не допускается.

При заполнении Паспорта ИСПДн категорически запрещается указание недостоверных или неполных сведений.

Вносимые в Паспорт ИСПДн данные должны строго соответствовать требованиям, предъявляемым к ним положениями настоящего Положения.

С целью уменьшения объема Паспорта ИСПДн допускается указание состава тех или иных данных

производить путем отсылки к его соответствующим разделам, в котором такие данные перечисляются. Оформление паспорта осуществляется в соответствии с приведенными в настоящем Положении формами.

4.6. Порядок создания, модернизации и ликвидации информационных систем персональных данных в ОУ

4.6.1. Порядок создания информационных систем персональных данных в ОУ

При возникновении необходимости в обработке персональных данных, для реализации заявленных в Уставе ОУ видов деятельности, создается информационная система персональных данных.

Запрещается создание информационной системы персональных данных, не соответствующей хотя бы одному из принципов, указанных в пункте 3.2 настоящего Положения.

Подразделение (должностное лицо), выступающее инициатором обработки персональных данных, при условии, что такая обработка не осуществляется в рамках обработки персональных данных в существующих информационных системах персональных данных, готовит проект Паспорта ИСПДн по установленному настоящим Положением образцу (Приложение 2).

Проект Паспорта ИСПДн в обязательном порядке согласовывается с заместителем Руководителя ОУ.

Утвержденный Паспорт ИСПДн является основанием для создания информационной системы персональных данных в ОУ.

По факту создания информационной системы персональных данных вносятся изменения в Перечень информационных систем персональных данных ОУ (пункт 4.7 настоящего Положения).

4.6.2. Порядок модернизации информационных систем персональных данных в ОУ

При возникновении необходимости внесения изменений в обработку персональных данных, в рамках существующих информационных систем персональных данных, осуществляется модернизация существующей информационной системы персональных данных.

В случае возникновения необходимости внесения изменений в обработку персональных данных в существующих информационных системах персональных данных, подразделение (должностное лицо), выступающее ответственным за осуществление такой обработки, готовит Проект о внесении изменений в существующий Паспорт ИСПДн.

Проект изменений в Паспорт ИСПДн в обязательном порядке согласовывается с заместителем Руководителя ОУ.

Утвержденный Паспорт ИСПДн с внесенными изменениями является основанием для создания или модернизации (изменения) информационной системы персональных данных.

4.6.3. Порядок ликвидации информационных систем персональных данных в ОУ

При возникновении необходимости в ликвидации информационной системы персональных данных, осуществляется комплекс мероприятий по уничтожению или передаче персональных данных в другие информационные системы персональных данных.

В случае возникновения необходимости в ликвидации информационной системы персональных данных, подразделение (должностное лицо), выступающее ответственным за ее ликвидацию, готовит План ликвидации информационной системы персональных данных, в котором определяет совершаемые при этом действия с персональными данными и их последовательность.

План ликвидации информационной системы персональных данных в обязательном порядке согласовывается с заместителем Руководителя ОУ.

Утвержденный Руководителем ОУ План ликвидации информационной системы персональных данных является основанием ликвидации информационной системы персональных данных.

По факту ликвидации информационной системы персональных данных вносятся изменения в Перечень информационных систем персональных данных ОУ (пункт 4.7 настоящего Положения).

4.7. Перечень информационных систем персональных данных в ОУ

Перечень информационных систем персональных данных определяется приказом Руководителя ОУ и оформляется в виде отдельного документа (или в виде дополнений или изменений к нему) – «Перечня информационных систем персональных данных ОУ».

Перечень информационных систем персональных данных ОУ храниться у заместителя Руководителя ОУ.

Форма «Перечня информационных систем персональных данных ОУ» устанавливается настоящим Положением (Приложение 3).

В Перечне информационных систем персональных данных должна содержаться следующая информация:

- наименование информационной системы персональных данных;
- цель создания/эксплуатации информационной системы персональных данных;
- перечень структурных подразделений, осуществляющих эксплуатацию информационной системы персональных данных;
- структурное подразделение, ответственное за эксплуатацию информационной системы персональных данных.

С «Перечнем информационных систем персональных данных» под роспись должны быть ознакомлены все руководители структурных подразделений ОУ.

Наименование и цель создания/эксплуатации информационной системы персональных данных должны совпадать с указанными в Паспорте на ИСПДн.

5. Конфиденциальность персональных данных

5.1. Режим ограниченного доступа к персональным данным в ОУ

С целью реализации требований действующего законодательства Российской Федерации в области персональных данных по обеспечению конфиденциальности персональных данных в ОУ вводится режим ограниченного доступа к персональным данным.

Создание режима ограниченного доступа к персональным данным включает в себя:

- создание и уточнение Перечня информации ограниченного доступа ОУ;
- создание и уточнение Положения о персональных данных в ОУ в части касающейся обеспечения конфиденциальности персональных данных и защиты информации, содержащей персональные данные;
- определение помещений, предназначенных для обработки персональных данных;
- определение должностных лиц допущенных к обработке персональных данных;
- определение технических средств обработки персональных данных;
- определение информационных ресурсов (информационных систем персональных данных, баз данных, массивов информации) содержащих персональные данные;
- создание комиссии по классификации и обследованию помещений, предназначенных для обработки персональных данных;
- создание актов классификации помещений, предназначенных для обработки персональных данных на предмет соответствия требованиям к инженерно-технической укреплённости по защите объектов от преступных посягательств;
- проведение мероприятий по обследованию помещений, предназначенных для обработки персональных данных, с составлением актов соответствия или проведением, при необходимости, доработок помещений по инженерно-технической укреплённости по защите объектов от преступных посягательств;
- дополнение в гражданско-правовые договоры с контрагентами по вопросам обязательства по обеспечению охраны конфиденциальности информации и ответственности за обеспечение охраны ее конфиденциальности;
- создание и ведение Журнал учета лиц (организаций), получивших доступ к персональным данным, и (или) лиц (организаций), которым такая информация была предоставлена или передана;
- дополнение должностных обязанностей (дополнения в трудовой договор работников), предусматривающие регулирование отношений по использованию информации, ограниченного доступа в ОУ;
- получение расписок ознакомлении работников, доступ которых к информации ограниченного доступа, обладателями которой являются ОУ, его контрагенты и клиенты, не обходим для выполнения им своих трудовых обязанностей, с перечнем информации ограниченного доступа, установленным режимом ограничения доступа к информации и мерами ответственности за его нарушение;
- заключение с работниками ОУ гражданских договоров об обязательстве выполнения установленного режима ограничения доступа к информации;
- не разглашении работниками ОУ информации ограниченного доступа, обладателями

которой является ОУ, в том числе и после прекращения или расторжения трудового договора;

- отказе работниками ОУ без согласия ОУ в использовании информации ограниченного доступа в личных целях;
- передаче (возврате) работниками ОУ при прекращении или расторжении трудового договора имеющиеся в пользовании работника материальных носителей информации, содержащих информацию ограниченного доступа такому ОУ;
- доработка обязанностей лица (структурного подразделения), ответственного за обеспечение режима ограничения доступа к информации в ОУ, в соответствии с внесением изменений в установленный режим;
- проведение начальных и периодических занятий и иных мероприятий по повышению уровня знаний работников, допущенных к информации ограниченного доступа в ОУ, по вопросам обеспечения режима ограничения доступа к информации в ОУ;
- получение расписок ознакомлении работников, доступ которых к информации ограниченного доступа, обладателями которой являются ОУ, его контрагенты и клиенты, не обходимо для выполнения им своих трудовых обязанностей, с действующим законодательством Российской Федерации по вопросам обеспечения безопасности информации, с эксплуатационной документацией на применяемые средства защиты информации, в том числе криптографические, в необходимом им для выполнения своих трудовых обязанностей объеме и другими документами, регламентирующими организацию и обеспечение безопасности информации ограниченного доступа при их обработке в информационных системах;
- создание и ведение Журнала регистрации машинных носителей информации;
- создание и ведение Журнала учета сейфов, металлических шкафов, спецхранилищ и ключей от них;
- создание и ведение списков лиц, имеющих доступ в помещения, в которых обрабатываются персональные данные;
- создание и ведение Журнала (-ов) приема (сдачи) под охрану помещений, в которых осуществляется обработка персональных данных;
- проектирование и реализация системы защиты персональных данных;
- документирование и реализация разрешительной системы доступа (матриц доступа) к информационным (программным) ресурсам в автоматизированных системах информационной системы персональных данных;
- создание и ведение списков лиц, допущенных к работе в информационных системах персональных данных;
- разработка инструкций о действиях работников, допущенных к обработке информации ограниченного доступа в ОУ с такой информацией (носителями) при возникновении чрезвычайных ситуаций (стихийных бедствий, техногенных катастроф, наводнений, пожаров, нарушениях правопорядка и др.);
- разработка инструкций для работников, допущенных к обработке информации ограниченного доступа в ОУ, по вопросам обеспечения безопасности персональных данных.

Выполнение указанных мероприятий и создание документов возлагается на структурные подразделения ОУ с обязательным согласованием принятых решений с руководством ОУ. Согласованные документы подлежат утверждению Руководителем ОУ.

5.2. Порядок учета и маркирования материальных носителей информации, образующихся в процессе обработки персональных данных

С целью реализации режима ограниченного доступа к персональным данным в ОУ и недопущению бесконтрольного использования машинных носителей, содержащих персональные данные вводится их поэкземплярный учет.

Учет машинных носителей, содержащих персональные данные, возлагается на Заместителя Руководителя ОУ.

Учет машинных носителей, содержащих персональные данные, осуществляется по Журналу учета машинных носителей информации. Форма «Журнала учета машинных носителей информации» устанавливается Техническим заданием на создание системы защиты персональных данных.

5.3. Порядок снятия режима конфиденциальности

В случаях, оговоренных настоящим Положением, допускается снятие режима конфиденциальности.

Снятие режима конфиденциальности осуществляется только на основании приказа Руководителя ОУ. Перед осуществлением операций по снятию режима конфиденциальности лица, их осуществляющие, обязаны убедиться, что все условия таких действий, оговоренные настоящим Положением и определенные действующим законодательством Российской Федерации, соблюдены.

6. Обеспечение безопасности персональных данных при их обработке

В соответствии с требованиями действующего законодательства в области персональных данных при обработке персональных данных ОУ обязано принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

Работы по обеспечению безопасности персональных данных при их обработке в информационных системах в ОУ являются неотъемлемой частью работ по созданию информационных систем.

6.1. Принципы обеспечения безопасности персональных данных при их обработке

Обеспечение безопасности персональных данных в ОУ должно осуществляться на основе следующих принципов:

- соблюдение конфиденциальности персональных данных и иных определенных в ОУ характеристик их безопасности;
- реализация права на доступ к персональным данным лиц, доступ которых к таким данным разрешается в рамках действующего законодательства Российской Федерации и локальными нормативными актами ОУ;
- обеспечение защиты информации, содержащей персональные данные, от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- проведение мероприятий, направленных на предотвращение несанкционированной передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных;
- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия.

Категорически запрещается нарушать указанные принципы по обеспечению безопасности персональных данных.

6.2. Требования по уровню обеспечения безопасности

С целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных, информационные системы персональных данных классифицируются в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Проведение классификации информационных систем включает в себя следующие этапы:

- сбор и анализ исходных данных по информационной системе;
- присвоение информационной системе соответствующего класса и его документальное

оформление.

При проведении классификации информационной системы учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);
- заданные характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- структура информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки персональных данных;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств информационной системы.

В случае выделения в составе информационной системы подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

Классификация информационных систем проводится на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем).

Результаты классификации информационных систем оформляются соответствующим Актом классификации.

6.3. Состав мероприятий по обеспечению безопасности персональных данных

Мероприятия по обеспечению безопасности персональных данных должны носить комплексный характер и включать в себя правовые, организационные и технические меры, описанные в настоящем Положении.

Порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются настоящим Положением.

6.3.1. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

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.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Ответственными за реализацию указанных мер являются руководители структурных подразделений ОУ.

6.3.2. Состав мероприятий по обеспечению безопасности персональных данных при их обработке, осуществляемой с использованием средств автоматизации

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных должны включать в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с

эксплуатационной и технической документацией;

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в информационной системе;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание системы защиты персональных данных.

К методам и способам защиты информации в информационных системах персональных данных относятся:

- методы и способы защиты информации, обрабатываемой техническими средствами информационной системы, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий (далее - методы и способы защиты информации от несанкционированного доступа);
- методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к персональным данным, результатом которого может стать копирование, распространение персональных данных, а также иных несанкционированных действий (далее - методы и способы защиты информации от утечки по техническим каналам).

Методами и способами защиты информации от несанкционированного доступа являются:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключаящее хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- использование защищенных каналов связи;
- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

В информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

При взаимодействии информационных систем с информационно-телекоммуникационными сетями

международного информационного обмена (сетями связи общего пользования) наряду с указанными методами и способами, основными методами и способами защиты информации от несанкционированного доступа являются:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- защита информации при ее передаче по каналам связи;
- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;
- использование средств антивирусной защиты;
- централизованное управление системой защиты персональных данных информационной системы.

Защита речевой информации и информации, представленной в виде информативных электрических сигналов и физических полей, осуществляется в случаях, когда при определении угроз безопасности персональных данных и формировании модели угроз применительно к информационной системе являются актуальными угрозы утечки акустической речевой информации, угрозы утечки видовой информации и угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.

Для исключения утечки персональных данных за счет побочных электромагнитных излучений и наводок в информационных системах I класса могут применяться следующие методы и способы защиты информации:

- использование технических средств в защищенном исполнении;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- размещение объектов защиты в соответствии с предписанием на эксплуатацию;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;
- обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

В информационных системах 2 класса для обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.

При применении в информационных системах функции голосового ввода персональных данных в информационную систему или функции воспроизведения информации акустическими средствами информационных систем для информационной системы I класса реализуются методы и способы защиты акустической (речевой) информации.

Методы и способы защиты акустической (речевой) информации заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе персональных данных в информационную систему или воспроизведении информации акустическими средствами.

Величина звукоизоляции определяется оператором исходя из характеристик помещения, его расположения и особенностей обработки персональных данных в информационной системе.

Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых

они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств, в том числе средств криптографической защиты информации.

6.4. Система защиты персональных данных

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Разработка системы защиты персональных данных, частных моделей угроз, моделей нарушителя осуществляется специализированной организацией на основании специального разрешения (лицензии) на осуществление данного вида деятельности.

6.4.1. Частные модели угроз и нарушителя

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем.

Под угрозами безопасности персональных данных при их обработке в информационной системе персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Частная модель угроз решает следующие задачи:

- анализ защищенности информационной системы персональных данных от угроз безопасности персональных данных в ходе учреждения и выполнения работ по обеспечению безопасности персональных данных;
- разработка системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационной системы персональных данных;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства информационной системы персональных данных, в результате которого может быть нарушено их функционирование;
- контроль обеспечения уровня защищенности персональных данных.

Частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных ОУ должна содержать систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных, обусловленных преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Частная модель угроз содержит единые исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационной системе персональных данных, связанным:

- с перехватом (съемом) персональных данных по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в информационной системы персональных данных с целью изменения, копирования, неправомерного распространения персональных данных или деструктивных воздействий на элементы информационной системы персональных данных и обрабатываемых в них персональных данных с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования персональных данных.

Состав и содержание угроз безопасности персональным данным определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным.

Совокупность таких условий и факторов формируется с учетом характеристик информационной системы персональных данных, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей и источников угроз.

При обеспечении безопасности персональных данных с использованием криптографических средств защиты информации производится нейтрализация атак, готовящимися и проводимыми нарушителями, причем возможности проведения атак обусловлены их возможностями. С учетом этого все возможные атаки определяются моделью нарушителя.

Модель нарушителя тесно связана с частной моделью угроз и, по сути, является ее частью. Смысловые отношения между ними следующие:

- в частной модели угроз содержится максимально полное описание угроз безопасности объекта;
- модель нарушителя содержит описание предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

6.4.2. Средства защиты информации

Средства защиты информации, применяемые в информационных системах персональных данных, в установленном порядке проходят процедуру оценки соответствия.

Технические и программные средства обработки персональных данных должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Эксплуатация средств защиты информации должна осуществляться строго в соответствии с эксплуатационной документацией на такие средства. Сотрудники ОУ, эксплуатирующие средства защиты информации должны быть ознакомлены с такой документацией под роспись.

6.5. Требования к помещениям, в которых производится обработка персональных данных

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

В ОУ специальное оборудование помещений, в которых ведется работа с персональными данными, осуществляется в соответствии с РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств».

Помещения, в которых располагаются технические средства информационных систем персональных данных или хранятся носители персональных данных, должны соответствовать требованиям пожарной безопасности, установленными действующим законодательством Российской Федерации.

В ОУ охрана помещений, в которых ведется работа с персональными данными, осуществляется в соответствии с локальными нормативными актами, разрабатываемыми службой безопасности.

Определение уровня специального оборудования помещения осуществляется специально создаваемой комиссией. По результатам определения класса и обследования помещения на

предмет его соответствия такому классу составляются Акты.

Кроме указанных мер по специальному оборудованию и охране помещений, в которых устанавливаются криптографические средства защиты информации или осуществляется их хранение, предъявляются дополнительные требования, определяемые методическими документами ФСБ России.

6.6. Требования к содержанию организационных мероприятий по обеспечению безопасности

Наряду с режимом ограничения доступа к персональным данным с целью обеспечения безопасности персональных данных в ОУ проводятся следующие мероприятия:

- создание и уточнение технологического паспорта, определяющего техническую составляющую информационных систем персональных данных;
- создание и уточнение технических паспортов на объекты информатизации, входящие в состав информационных систем персональных данных;
- разрабатываются инструкции по конкретизации отдельных действий, направленных на обеспечение безопасности персональных данных;
- создание комиссии по классификации информационных систем персональных данных;
- создание актов классификации информационных систем персональных данных.

Состав организационных мероприятий по обеспечению безопасности персональных данных может уточняться в зависимости от конкретных условий функционирования информационных систем персональных данных в ОУ.

Разработка, согласование и утверждение указанных документов осуществляется аналогично документам, создаваемым в рамках режима ограничения доступа к персональным данным.

6.7. Требования к персоналу, задействованному в обработке персональных данных

Лица, доступ которых к персональным данным, обрабатываемым в информационных системах ОУ, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного Руководителем ОУ.

Лица, обрабатывающие персональные данные обязаны:

- знать и выполнять действующее законодательство в области персональных данных;
- знать и выполнять локальные нормативные документы ОУ по вопросам обработки и обеспечения безопасности персональных данных;
- правильно эксплуатировать средства защиты информации, в соответствии с документацией к ним.

6.8. Требования к порядку передачи (пересылки) носителей информации, содержащих персональные данные

Передача (пересылка) носителей информации, содержащих персональные данные должна осуществляться способом, исключающим несанкционированный доступ к такой информации. Факт передачи (пересылки) таких носителей должна оформляться в Журнале учета лиц (организаций), получивших доступ к персональным данным, и (или) лиц (организаций), которым такая информация была предоставлена или передана.

6.9. Требования к техническим средствам, системному программному обеспечению и их настройкам

Требования к техническим средствам, системному программному обеспечению и их настройкам определяются требованиями документов по оценке соответствия средств защиты информации, заводской и эксплуатационной документации на них.

6.10. Регламент оценки соответствия требованиям по безопасности информации

Порядок оценки соответствия информационных систем персональных данных требованиям безопасности информации осуществляется в порядке, определяемом действующим законодательством Российской Федерации и Программой такой оценки. Программу проведения оценочных испытаний разрабатывает организация, проводящая такую оценку. Программа согласовывается с ОУ.

Программа оценки соответствия информационных систем персональных данных требованиям безопасности информации должна содержать:

- перечень работ и их продолжительность;

- методики испытаний (или используются типовые методики);
- количественный и профессиональный состав оценочной комиссии;
- необходимость использования контрольной аппаратуры и тестовых средств.

Порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, соответствия их установленным требованиям, а также применяемые в этих целях контрольная аппаратура и тестовые средства определяются в методиках испытаний различных видов объектов информатизации.

По результатам оценки соответствия информационных систем персональным данным требованиям безопасности информации оформляются протоколы и заключение о соответствии таким требованиям. На основании заключения, в случае получения положительного решения о соответствии информационной системы персональным данным предъявляемым требованиям по обеспечению безопасности персональных данных, оформляется документ, подтверждающий выполнение требований по безопасности информации.

7. Порядок контроля за соблюдением требований по обработке и обеспечению безопасности персональных данных

7.1. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности данных

С целью соблюдения законности обработки и обеспечения безопасности персональных данных в ОУ проводится периодический контроль за соблюдением установленных требований по данным вопросам. Контроль за исполнением нормативных актов ОУ по вопросам обработки и обеспечения безопасности персональных данных возлагается на заместителя Руководителя ОУ.

Основными вопросами внутреннего контроля являются:

- соответствие документации по вопросам персональных данных реальному положению дел;
- соблюдение лицами, допущенными к обработке персональных данных, всех требований, установленных локальными нормативными актами по вопросам персональных данных в ОУ.
- проверка соблюдения защиты прав субъектов персональных данных, путем анализа их обращений и действий совершаемыми сотрудниками ОУ в связи с этими обращениями.

7.2. Порядок внешнего контроля за соблюдением требований по обработке и обеспечению безопасности данных

Законодательство в области персональных данных определяет следующие контролирующие органы по вопросам обработки и обеспечения безопасности персональных данных:

- уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства в области персональных данных, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи;
- контроль и надзор за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

Порядок проведения контроля устанавливается соответствующими административными регламентами. При этом уполномоченный орган по защите прав субъектов персональных данных имеет право:

- запрашивать информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
- осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;
- требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;
 - обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде;
 - направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;
 - направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;
 - привлекать к административной ответственности лиц, виновных в нарушении законодательства в области персональных данных.
- Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

8. Ответственность за нарушение норм, регулирующих обработку персональных данных

Лица, допустившие нарушения правил обработки или обеспечения безопасности персональных данных несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

9. Мероприятия при возникновении обстоятельств непреодолимой силы (форс-мажор)

В случае возникновения обстоятельств непреодолимой силы, возникших в результате событий чрезвычайного характера, которые ОУ не могло предвидеть и предотвратить разумными мерами, должностные лица ОУ обязаны принять все возможные меры по недопущению нарушения прав субъектов персональных данных.

К обстоятельствам непреодолимой силы относятся события, на которые ОУ не могло оказывать влияние и за возникновение которых оно не несет ответственности: землетрясение, наводнение, пожар, забастовки, насильственные или военные действия любого характера, решения органов государственной власти препятствующие исполнению требований законодательства в области персональных данных.

Надлежащим доказательством наличия указанных выше обстоятельств будут служить официальные документы ОУ и органов государственной власти Российской Федерации.

ОУ в случае возникновения указанных выше обстоятельств и нарушении прав субъектов персональных данных, связанных с такими обстоятельствами, обязано известить субъектов персональных данных любым доступным способом.

10. Мероприятия по обработке персональных данных при ликвидации или реорганизации ОУ

При ликвидации ОУ все носители персональных данных подлежат уничтожению установленным настоящим Положением способом, за исключением носителей, подлежащих в соответствии с действующим законодательством Российской Федерации передаче в организацию-учредитель ОУ.

При реорганизации ОУ в форме слияния, присоединения и преобразования решение о необходимости уничтожения персональных данных или передаче их вновь образуемому образовательному учреждению принимается в соответствии с действующим законодательством Российской Федерации.

11. Приложения

- Приложение 1. Перечень документов по разработке Положения о персональных данных в ОУ
- Приложение 2. Форма юридического паспорта информационной системы персональных данных
- Приложение 3. Форма Перечня информационных систем персональных данных
- Приложение 4. Форма Согласия на обработку персональных данных
- Приложение 5. Форма Согласия субъекта персональных данных на запрос его персональных

данных у третьих лиц

- Приложение 6. Форма журнала учета лиц (организаций), получивших доступ к персональным данным, и (или) лиц (организаций), которым такая информация была предоставлена или передана
- Приложение 7. Форма акта уничтожения персональных данных субъектов персональных данных по достижении цели обработки, внесения изменений, блокировки и т.д.
- Приложение 8. Форма уведомлений о совершенных операциях над персональными данными

**Перечень документов по разработке
Положения о персональных данных в ОУ**

- 1. Документы по вопросам защиты прав субъектов персональных данных.**
 - 1.1. Общие документы.**
 - 1.1.1. Федеральный Закон РФ №152-ФЗ от 27.07.2006 г. «О персональных данных».
 - 1.1.2. Федеральный закон №63-ФЗ от 13.06.96 г. «Уголовный кодекс Российской Федерации».
 - 1.1.3. Федеральный закон №195-ФЗ от 30.12.01 г. «Кодекс Российской Федерации об административных правонарушениях».
 - 1.2. Документы Министерства связи РФ.**
 - 1.2.1. «Административный регламент проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных» Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций № 630 от 01.12.2009 г.
 - 1.2.2. Приказ Россвязьохранкультуры №154 от 28.03.08 г. «Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных».
 - 1.2.3. Приказ Россвязькомнадзора «Об утверждении образца формы уведомления об обработке персональных данных».
- 2. Документы по вопросам деятельности учреждения.**
 - 2.1. Общие документы.**
 - 2.1.1. Федеральный Закон РФ №197-ФЗ от 30.12.2001 г. «Трудовой кодекс Российской Федерации».
 - 2.1.2. Постановление Государственного комитета Российской Федерации по статистике №1 от 05.01.2004 г. «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты».
 - 2.1.3. Федеральный Закон РФ №117-ФЗ от 05.08.2000 г. «Налоговый кодекс Российской Федерации часть первая».
 - 2.1.4. Федеральный Закон РФ №146-ФЗ от 31.07.1998 г. «Налоговый кодекс Российской Федерации часть вторая».
 - 2.1.5. Федеральный Закон РФ №129-ФЗ от 21.11.1996 г. «О бухгалтерском учете».
- 3. Документы по вопросам защиты информации.**
 - 3.1. Общие документы.**
 - 3.1.1. Федеральный Закон РФ №149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации».
 - 3.1.2. Федеральный Закон РФ №98-ФЗ от 29.07.2004 г. «О коммерческой тайне».
 - 3.1.3. Постановление Правительства РФ №35 от 05 декабря 1991 г. «О перечне сведений, которые не могут составлять коммерческую тайну».
 - 3.1.4. Федеральный Закон РФ №1-ФЗ от 10.01.2002 г. «Об электронной цифровой подписи».
 - 3.1.5. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
 - 3.1.6. Приказ Федеральной службы по техническому и экспортному контролю №55 Федеральной службы безопасности Российской Федерации №86 Министерства информационных технологий и связи Российской Федерации №20 от 13.02.2008 г. «Об утверждении порядка проведения классификации информационных систем персональных данных».
 - 3.1.7. Постановление Правительства РФ №781 от 17.11.2007 г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
 - 3.1.8. Постановление Правительства РФ №687 от 15.09.2008 г. «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3.1.9. Постановление Правительства РФ №512 от 06.07.2008 г. «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

3.1.10. Постановление Правительства РФ 125 от 04.03.2010 г. «О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию».

3.2. Документы ФСТЭК РФ.

3.2.1. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» Федеральной службы по техническому и экспортному контролю от 14.02.2008 г.

3.2.2. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» Федеральной службы по техническому и экспортному контролю от 15.02.2008 г.

3.2.3. Приказ Федеральной службы по техническому и экспортному контролю №58 от 5.02.2010 г. «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

3.2.4. Нормативно-методический документ. «Специальные требования и рекомендации по технической защите конфиденциальной информации». Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

3.2.5. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Гостехкомиссия России, 1992.

3.2.6. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Приказ Гостехкомиссии России, 1992.

3.2.7. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1992.

3.2.8. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, 1992.

3.2.9. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1997.

3.2.10. Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей. Приказ Гостехкомиссии России от 4 июня 1999 г. № 114.

3.2.11. «Методические рекомендации по технической защите информации, составляющей коммерческую тайну».

3.2.12. «Пособия к методическим рекомендациям по технической защите информации, составляющей коммерческую тайну».

3.2.13. «Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам», Гостехкомиссия России, Москва, 2002.

3.2.14. «Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах», Гостехкомиссия России, Москва, 2002.

3.2.15. «Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации», Гостехкомиссия России, Москва, 2002.

3.2.16. «Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации», Гостехкомиссия России, Москва, 2002.

3.3. Документы ФСБ РФ.

3.3.1. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с ис-

пользованием средств автоматизации» руководства 8 Центра ФСБ России № 149/54-144 от 21.02.2008 г.

3.3.2. «Типовые требования по учреждению и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» руководства 8 Центра ФСБ России № 149/6/6-622 от 21.02.2008 г.

3.3.3. Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации №152 от 13.06.2001 г. «Об утверждении инструкции об учреждении и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

3.3.4. Приказ Федеральной службы безопасности Российской Федерации №66 от 09.02.2005 г. «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)».

3.3.5. «Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» Руководства 8 Центра ФСБ России № 149/7/2/6-1173 от 08.08.2009.

3.3.6. Указ Президента РФ №334 от 03.04.95 г. «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».

3.4. Документы МВД РФ.

3.4.1. «РД 78.36.003-2002 Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств» Министерства внутренних дел Российской Федерации, Главного управления вневедомственной охраны от 06.11.2002 г.

3.5. Документы Министерства связи РФ.

3.5.1. Постановление Правительства Российской Федерации №424 от 18.05.2009 г. «Об особенностях подключения федеральных государственных систем к информационно-телекоммуникационным сетям».

3.5.2. Приказ Министерства связи и массовых коммуникаций Российской Федерации №104 от 25.08.2009 г. «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования».

3.5.3. Приказ ФСБ РФ и Федеральной службы по техническому и экспортному контролю №416/489 от 31 августа 2010 г. «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»

4. Документы по вопросам лицензирования.

4.1. Общие документы.

4.1.1. Закон Российской Федерации от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности».

4.1.2. Постановление Правительства РФ №326 от 11.04.2000 «О лицензировании отдельных видов деятельности».

4.1.3. Постановление Правительства Российской Федерации от 26 января 2006 г. № 45 «Об учреждении лицензирования отдельных видов деятельности».

4.1.4. Постановление Правительства Российской Федерации от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».

4.1.5. Постановление Правительства Российской Федерации от 31 августа 2006 г. № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

4.2. Документы ФСТЭК РФ.

4.2.1. «Положение о государственном лицензировании деятельности в области защиты информации», решение Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации №10 от 27.04.94 г.

4.2.2. Приказ ФСТЭК РФ №181 от 28.08.07 «Об утверждении административного Регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной

функции по лицензированию деятельности по технической защите конфиденциальной информации».

4.2.3. Приказ ФСТЭК РФ №182 от 28.08.07 «Об утверждении административного Регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

4.3. Документы ФСБ РФ.

4.3.1. Постановление Правительства Российской Федерации №957 от 29.12.07 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».

4.3.2. Приказ ФСБ России №104 от 16.03.09 «Об утверждении административного Регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по предоставлению услуг в области шифрования информации».

4.3.3. Приказ ФСБ России №105 от 16.03.09 «Об утверждении административного Регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по техническому обслуживанию шифровальных (криптографических) средств».

4.3.4. Приказ ФСБ России №106 от 16.03.09 «Об утверждении административного Регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по распространению шифровальных (криптографических) средств».

5. Документы по вопросам сертификации.

5.1. Документы ФСТЭК РФ.

5.1.1. Постановление Правительства РФ №608 от 26.06.95 г. «О сертификации средств защиты информации».

5.1.2. «Положение о сертификации средств защиты информации по требованиям безопасности информации», приказ Председателя Гостехкомиссии России №199 от 27.10.95 г.

5.1.3. Положение по аттестации объектов информатизации по требованиям безопасности информации, утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.94 г.

5.1.4. Постановление Правительства РФ № 330 от 15 мая 2010 г. «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг)»

6. Документы архивного делопроизводства.

6.1.1. Федеральный закон № 125 от 22.10.04 «Об архивном фонде Российской Федерации и архивах».

6.1.2. Общероссийский классификатор управленческой документации ОК 011-93, утвержденный Постановлением Госстандарта РФ от 30 декабря 1993 г. №299

6.1.3. Приказ Министерства культуры РФ от 25 августа 2010 г. №558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»

6.1.4. Приказ Министерства культуры и массовых коммуникаций РФ от 31 июля 2007 г. №1182 «Об утверждении Перечня типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения»

6.1.5. ГОСТ Р 51141-98 Делопроизводство и архивное дело. Термины и определения.

7. Документы других организаций.

7.1.1. Приказ Министерства здравоохранения и социального развития РФ №205 от 22.04.09 г. «Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей руководителей и

специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации».

8. ГОСТ.

8.1.1. ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.

8.1.2. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

8.1.3. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

8.1.4. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

8.1.5. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

8.1.6. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

8.1.7. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения

8.1.8. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования

8.1.9. РД 50-682-89. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Основные положения.

8.1.10. РД 50-34.698-90. Методические указания. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов.

8.1.11. РД 50-680-88. Методические указания. Автоматизированные системы. Основные положения

8.1.12. ГОСТ Р 50-34.119-90. Рекомендации. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Архитектура локальных вычислительных сетей.

8.1.13. ГОСТ 24.208-80 Требования к содержанию документов стадии «Ввод в эксплуатацию».

8.1.14. ГОСТ 2.118-73 Техническое предложение.

8.1.15. ГОСТ 2.119-73 Эскизный проект.

8.1.16. ГОСТ 2.120-73 Технический проект.

8.1.17. ГОСТ 2.601-95 Эксплуатационные документы автоматизации. Общие положения.

8.1.18. ГОСТ ИСО/МЭК 15408-1-2002. Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

8.1.19. ГОСТ ИСО/МЭК 15408-2-2002. Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий Часть 2. Функциональные требования безопасности.

8.1.20. ГОСТ ИСО/МЭК 15408-3-2002. Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

8.1.21. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

8.1.22. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.

8.1.23. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер.

8.1.24. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети.

8.1.25. ГОСТ Р ИСО/МЭК 13569-xxxx (проект 10.05.2007) Финансовые услуги. Рекомендации по информационной безопасности.

8.1.26. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.

- 8.1.27. ГОСТ Р ИСО/МЭК 18044 (проект) Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.
- 8.1.28. ГОСТ Р ИСО/МЭК 18045 (проект) Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.
- 8.1.29. ГОСТ Р ИСО/МЭК 19794-5-2006 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица.
- 8.1.30. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
- 8.1.31. ГОСТ Р 50.1.056 Техническая защита информации. Основные термины и определения.
- 8.1.32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.
- 8.1.33. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
- 8.1.34. ГОСТ Р 52069.0-2003 Защита информации. Система стандартов. Основные положения.
- 8.1.35. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества.

Приложение 2. Форма юридического паспорта информационной системы
персональных данных

Приложение 2.

**Форма юридического паспорта
информационной системы персональных данных**

Утверждаю

[Наименование должности руководителя
образовательного учреждения]

[полное наименование образовательного
учреждения]

_____ [Инициалы и фамилия]

«_____» _____ 20__ г.

**Юридический паспорт
информационной системы персональных данных**
федерального государственного бюджетного образовательного учреждения высшего
профессионального образования «Омский государственный педагогический
университет»

[наименование информационной системы персональных данных]

Разработал

[Наименование должности руководителя
образовательного учреждения]

[полное наименование образовательного
учреждения]

_____ [Инициалы и фамилия]

«_____» _____ 2010 г.

[Город]

Содержание

1. Наименование информационной системы персональных данных

Полное наименование информационной системы персональных данных (далее – ИСПДн): информационная система персональных данных (далее – ИСПДн) [полное наименование ИСПДн].

Сокращенное наименование ИСПДн: ИСПДн [сокращенное наименование ИСПДн].

Примечание: в данном разделе указывается наименование информационной системы персональных данных (далее – ИСПДн), которое должно отражать основное назначение данной информационной системы либо наименование программных средств обработки персональных данных в данной ИСПДн.

2. Цели создания или эксплуатации ИСПДн

Цель создание и эксплуатации ИСПДн [наименование ИСПДн] – [описание (перечисление) целей создания ИСПДн].

Примечание: в данном разделе определяются цели создания и эксплуатации ИСПДн. При этом указываются предполагаемое назначение ИСПДн, в соответствии с предлагаемыми потребителям услугами, осуществляемыми ИСПДн внутренними задачами или с определенными требованиями, предъявляемыми действующим в Российской Федерации законодательством. Цель создания и эксплуатации ИСПДн должна соответствовать заявленным в Уставе видам деятельности.

3. Структурное подразделение, ответственное за эксплуатацию ИСПДн

Структурным подразделением ОУ (должностным лицом), ответственным за эксплуатацию ИСПДн [наименование ИСПДн] является: [наименование подразделения]

Примечание: в данном разделе указывается подразделение (должностное лицо), назначенное ответственным за создание и эксплуатацию ИСПДн в части обработки в ней персональных данных.

4. Цель обработки персональных данных в информационной системе персональных данных

Перечень структурных подразделений, осуществляющих обработку персональных данных в ИСПДн [наименование ИСПДн] и перечень целей обработки персональных данных в них (задач для каждого указанного структурного подразделения, в рамках которых производится обработка персональных данных в ИСПДн [наименование ИСПДн]) приведены в таблице 1.

Таблица 1. Цель обработки персональных данных в информационной системе персональных данных.

№ п/п	Наименование структурного подразделения	Цель обработки персональных данных в соответствии с Уставом ОУ	Частная цель обработки персональных данных в соответствии положением о структурном подразделении
1.			

Примечание: при определении целей обработки персональных данных в ИСПДн указываются:

- *перечень структурных подразделений, осуществляющих обработку персональных данных в информационной системе персональных данных;*
- *перечень целей обработки персональных данных для каждого указанного структурного подразделения, в рамках которых производится обработка персональных данных в информационной системе персональных данных (в соответствии с видами деятельности, заявленными в учредительных документах ОУ);*
- *перечень целей обработки персональных данных для каждого указанного структурного подразделения, в рамках которых производится обработка персональных данных в информационной системе персональных данных (в соответствии с задачами или функциями структурного подразделения ОУ, указанными в положении о таком структурном подразделении).*

5. Способы обработки персональных данных

Способы обработки персональных данных при решении заявленных целей в каждом структурном подразделении приведены в таблице 2.

Таблица 2. Способы обработки персональных данных

№ п/п	Наименование структурного подразделения	Цель обработки персональных данных	Способы обработки персональных данных
1.			

Примечание: в данном разделе указываются:

- *заявленные цели обработки персональных данных, в рамках которых производится обработка персональных данных в информационной системе персональных данных в каждом структурном подразделении (в соответствии с видами деятельности, заявленными в учредительных документах ОУ и задачами или функциями структурного подразделения ОУ, указанными в положении о таком структурном подразделении);*

– способы обработки персональных данных в рамках каждой из заявленных задач обработки персональных данных в информационной системе персональных данных.

6. Перечень идентификаторов персональных данных о субъекте персональных данных, обрабатываемых в информационной системе персональных данных

Перечни идентификаторов персональных данных, используемые для решения задач и функций структурными подразделениями, приведены в таблице 3.

Таблица 3. Перечни идентификаторов персональных данных, используемые для решения задач и функций структурными подразделениями

№ п/п	Наименование структурного подразделения	Цель обработки персональных данных	Перечни идентификаторов персональных данных	Статус персональных данных (категория)
1.				

Примечание: в данном разделе указываются:

- заявленные цели обработки персональных данных, в рамках которых производится обработка персональных данных в информационной системе персональных данных в каждом структурном подразделении (в соответствии с видами деятельности, заявленными в учредительных документах ОУ и задачами или функциями структурного подразделения ОУ, указанными в положении о таком структурном подразделении);
- все наборы идентификаторов персональных данных принадлежащих субъекту персональных данных, обрабатываемых в информационной системе персональных данных, включая внутренние идентификаторы, принятые в ОУ для каждой заявленной цели обработки персональных данных или для группы таких целей;
- для каждого набора персональных данных определяется их статус (категория) в соответствии с Положением о персональных данных.

7. Необходимость и правовое основание обработки персональных данных в информационной системе персональных данных

Необходимость обработки персональных данных в ИСПДн [наименование ИСПДн] в зависимости от целей обработки персональных данных в каждом структурном подразделении с ее документальным основанием приведена в таблице 5.

Таблица 5. Необходимость обработки персональных данных в ИСПДн [наименование ИСПДн]

№ п/п	Наименование структурного подразделения	Цель обработки персональных данных	Вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, в том числе локального определяющего <u>необходимость</u> обработки персональных данных в ИСПДн	Вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, в том числе локального определяющего <u>правовое основание</u> обработки персональных данных в ИСПДн
1.				

Примечание: в данном разделе определяется:

– заявленные цели обработки персональных данных, в рамках которых производится обработка персональных данных в информационной системе персональных данных в каждом структурном подразделении (в соответствии с видами деятельности, заявленными в учредительных документах ОУ и задачами или функциями структурного подразделения ОУ, указанными в положении о таком структурном подразделении);

– вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, в том числе локального, определяющего необходимость обработки персональных данных;

– вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, в том числе локального, определяющего правовое основание обработки персональных данных.

В случае наличия нескольких нормативно-правовых актов, определяющих необходимость обработки персональных данных или правовое основание такой обработки, необходимо указывать их все в порядке убывания юридической силы (например, федеральный закон, постановление Правительства РФ, локальный нормативный акт и т.п.).

Необходимость обработки персональных данных определяется заявленными целями обработки таких данных (технологическим процессом или регламентов выполняемых операций в рамках деятельности учреждения). Необходимость обработки персональных данных может определяться как требованием нормативно-правовых актов, так и внутренними документами ОУ.

Определение правовых оснований на обработку персональных данных осуществляется с целью определения законности обработки персональных данных. Законность обработки персональных данных может определяться как нормативно-правовым актом, так и виде документа, определяющего согласие субъекта персональных данных на обработку его персональных данных, в случае, если необходимость обработки персональных данных определяется самим ОУ (например, в виде согласия на обработку персональных данных или договора, одной из сторон которого является субъект персональных данных).

8. Необходимость получения согласия субъекта персональных данных на обработку его персональных данных

Необходимость получения согласия субъекта персональных данных на обработку его персональных данных в зависимости от целей обработки персональных данных в каждом структурном подразделении с ее документальным основанием приведена в таблице 6.

Таблица 6. Необходимость получения согласия субъекта персональных данных.

№ п/п	Наименование структурного подразделения	Цель обработки персональных данных	Особенности обработки персональных данных*	Необходимость получения согласия субъекта персональных данных на обработку его персональных данных	Основание (ссылка на пункт Федерального закона №152-ФЗ «О персональных данных»)
1.					

Примечание: в данном разделе определяется:

– заявленные цели обработки персональных данных, в рамках которых производится обработка персональных данных в информационной системе персональных данных в каждом структурном подразделении (в соответствии с видами деятельности, заявленными в учредительных документах ОУ и задачами или функциями структурного подразделения ОУ, указанными в положении о таком структурном подразделении);

– на основании ранее определенных данных определяются особенности обработки персональных данных для каждой заявленной цели обработки персональных данных: обработка персональных данных с использованием средств автоматизации; исключительно автоматизированная обработка персональных данных; обработка специальных категорий персональных данных; обработка биометрических персональных данных; обработка общедоступных персональных данных; обработка персональных данных с целью однократного пропуска субъекта персональных данных на охраняемую территорию; обработка персональных данных при трансграничной передаче персональных данных; поручение обработки персональных данных другому лицу; обезличивание персональных данных; обработка персональных данных в целях продвижения товаров, работ, услуг на рынке (при наличии нескольких особенностей обработки персональных данных указываются они все);

– для каждой заявленной цели обработки персональных данных на основании статей Федерального закона №152-ФЗ «О персональных данных» определяется необходимость получения согласия субъекта персональных данных на обработку его персональных данных, а так же

делается ссылка на пункт и статью указанного закона.

9. Юридические последствия, порождаемые в результате действий (операций) с персональными данными, в отношении субъекта персональных данных либо иным образом затрагивающих права и свободы субъекта персональных данных

Юридические последствия, порождаемые в результате действий (операций) с персональными данными, в отношении субъекта персональных данных либо иным образом затрагивающих права и свободы субъекта персональных данных приведены в таблице 7.

Таблица 7. Юридические последствия, порождаемые в результате действий (операций) с персональными данными, в отношении субъекта персональных данных либо иным образом затрагивающих права и свободы субъекта персональных данных

№ п/п	Наименование структурного подразделения	Цель обработки персональных данных	Юридические последствия
1.			

Примечание: в данном разделе перечисляются:

- заявленные цели обработки персональных данных, в рамках которых производится обработка персональных данных в информационной системе персональных данных в каждом структурном подразделении (в соответствии с видами деятельности, заявленными в учредительных документах ОУ и задачами или функциями структурного подразделения ОУ, указанными в положении о таком структурном подразделении);
- все юридические последствия в отношении субъекта персональных данных, порождаемые принятием решения на основании использования персональных данных или совершением иных действий с его персональными данными, при выполнении каждой из заявленных целей обработки персональных данных.

10. Круг субъектов, персональные данные которых подлежат обработке в информационной системе персональных данных

Круг субъектов, персональные данные которых, подлежат обработке в информационной системе персональных данных приведены в таблице 8.

Таблица 8. Круг субъектов, персональные данные которых, подлежат обработке в информационной системе персональных данных

№ п/п	Наименование структурного подразделения	Цель обработки персональных данных	Круг субъектов, персональные данные которых подлежат обработке в информационной системе персональных данных
1.			

№ п/п	Наименование структурного подразделения	Цель обработки персональных данных	Круг субъектов, персональные данные которых подлежат обработке в информационной системе персональных данных

Примечание: в данном разделе указываются:

- заявленные цели обработки персональных данных, в рамках которых производится обработка персональных данных в информационной системе персональных данных в каждом структурном подразделении (в соответствии с видами деятельности, заявленными в учредительных документах ОУ и задачами или функциями структурного подразделения ОУ, указанными в положении о таком структурном подразделении);
- круг субъектов, персональные данные которых подлежат обработке в информационной системе персональных данных (признак, объединяющий определенную группу граждан, находящихся в рамках гражданских отношений с ОУ) субъектов персональных данных, персональные данные которых подлежат обработке, по критериям целей обработки персональных данных (например, «работники», «учащиеся» и т.п.).

11. Количество субъектов персональных данных, чьи персональные данные обрабатываются

В информационной системе персональных данных обрабатываются персональные данные [количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн] субъектов персональных данных в [признак группировки субъектов персональных данных].

Примечание: в данном разделе указываются:

- количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн: более чем 100 000, от 1000 до 100 000, менее чем 1000;
- признак группировки субъектов персональных данных: в пределах субъекта Российской Федерации или Российской Федерации в целом, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования, в пределах конкретной учреждения.

12. Действия (операции) с персональными данными в информационной системе персональных данных

Действия (операции) с персональными данными в информационной системе персональных данных приведены в таблице 9.

Таблица 9. Действия (операции) с персональными данными в информационной системе персональных данных

Полномочия по выполнению действий (операций) с персональными данными	Группы должностей, обладающих указанными полномочиями

Примечание: в данном разделе должны быть перечислены (отмечены) все реально производимые действия (операции) с персональными данными при их обработке в ИСПДн (наименование таких действий (операций) должны соответствовать Положению о Персональных данных) и соответствующие им должности или группы должностей, обладающих указанными полномочиями, позволяющие осуществлять данные операции.

13. Способы и источники получения персональных данных

Способы и источники получения персональных данных для ввода их в информационную систему для реализации заявленных целей их обработки приведены в таблице 10.

Таблица 10. Способы и источники получения персональных данных

№ п/п	Наименование структурного подразделения	Цель обработки персональных данных	Источник получения	Способы получения
1.				

Примечание: в данном разделе указываются:

- *заявленные цели обработки персональных данных, в рамках которых производится обработка персональных данных в информационной системе персональных данных в каждом структурном подразделении (в соответствии с видами деятельности, заявленными в учредительных документах ОУ и задачами или функциями структурного подразделения ОУ, указанными в положении о таком структурном подразделении);*
- *источники получения персональных данных субъекта персональных данных для каждой цели обработки персональных данных (например, работники ОУ, учащиеся ОУ, родители учащихся ОУ и др.);*
- *способы получения персональных данных субъекта персональных данных для каждого источника или группы источников получения персональных данных (например, непосредственно от субъекта персональных данных, от Комитета образования и науки Курской области и др.).*

14. Способы передачи персональных данных и их получатели

Способы передачи персональных данных из информационной системы персональных данных и их получатели приведены в таблице 10.

Таблица 11. Способы передачи персональных данных и их получатели

№ п/п	Наименование структурного подразделения	Цель обработки персональных данных	Куда передаются	Способы передачи	Вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, в том числе локального определяющего <u>правовое основание</u> передачи персональных данных
1.					

Примечание: в данном разделе указываются:

- заявленные цели обработки персональных данных, в рамках которых производится обработка персональных данных в информационной системе персональных данных в каждом структурном подразделении (в соответствии с видами деятельности, заявленными в учредительных документах ОУ и задачами или функциями структурного подразделения ОУ, указанными в положении о таком структурном подразделении);
- перечень организаций-получателей персональных данных, которым осуществляется их передача для каждой цели обработки персональных данных;
- способы передачи персональных данных субъекта персональных данных для каждой указанной организации-получателя персональных данных;
- вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, в том числе локального, или договора, определяющего правовое основание для передачи персональных данных.

15. Определение сроков обработки, в том числе хранения персональных данных в ИСПДн

Сроки обработки персональных данных субъектов персональных данных в рамках деятельности образовательного учреждения определяются требованиями [вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, в том числе локального, определяющего сроки обработки персональных данных] и составляют не менее [указывается максимальный срок хранения данных] [с какого момента исчисляется срок].

Сроки обработки персональных данных субъектов персональных данных в рамках деятельности ОУ как работодателя и собственника обособленного имущества определяются требованиями [вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, в том числе локального, определяющего сроки обработки персональных данных].

Примечание: в данном разделе указываются:

– вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, в том числе локального, определяющего сроки обработки персональных данных для каждого направления деятельности учреждения и конкретные сроки хранения документов. В случае указания документа, устанавливающего сроки хранения перечня документов, образующихся в процессе деятельности учреждения, допускается указывать только сведения о таком документе, без указания конкретных сроков.

16. Юридические последствия отказа в предоставлении своих персональных данных

Юридические последствия отказа в предоставлении своих персональных данных приведены в таблице 12.

Таблица 12. Юридические последствия отказа в предоставлении своих персональных данных

№ п/п	Случаи обязательного предоставления своих персональных данных субъектом персональных данных	Вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, устанавливающего обязательность предоставления своих персональных данных субъектом персональных данных	Юридические последствия отказа в предоставлении своих персональных данных (ссылка на статью, пункт нормативно-правового акта)
1.			

Примечание: в данном разделе перечисляются:

– все случаи обязательного предоставления субъектом персональных данных своих персональных данных, для занесения их в ИСПДн;

– вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, устанавливающего обязательность предоставления своих персональных данных субъектом персональных данных;

– юридические последствия отказа предоставить свои персональные данные для каждого случая обязательного предоставления субъектом персональных данных своих персональных данных (к таким последствиям могут относиться: отказ в открытии счета (вклада) (в связи с запретом осуществления такой операции, установленным федеральным законом); отказ в принятии на работу, в связи с невозможностью оформления трудовых отношений в соответствии с требованиями трудового законодательства; и другие).

17. Заданные характеристики безопасности обрабатываемых в информационной системе персональных данных

Заданные характеристики безопасности персональных данных при обработке их в информационной системе персональных данных

приведены в таблице 13.

Таблица 13. Заданные характеристики безопасности персональных данных

№ п/п	Вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, в том числе локального характеристики безопасности персональных данных при обработке их в ИСПДн	Ссылка на статью (пункт) нормативно-правового акта, в том числе локального определяющей характеристики безопасности персональных данных при обработке их в ИСПДн	Характеристики безопасности персональных данных
1.			

Примечание: в данном разделе указываются:

- вид, издавший орган, номер, дата принятия и наименование нормативно-правового акта, в том числе локального, задающего характеристики безопасности персональных данных при обработке их в ИСПДн;
- ссылка на статью (пункт) документа, установившего такое требование;
- заданные характеристики безопасности персональных данных (обеспечение конфиденциальности, защищенности от уничтожения, изменения, блокирования, а также иных несанкционированных действий с информацией, содержащей персональные данные).

18. Места обработки персональных данных

Обработка персональных данных о субъектах персональных данных в ИСПДн [наименование ИСПДн] осуществляется техническими средствами по следующим адресам:

- [наименование офиса]: [почтовый адрес];
-

Примечание: в данном разделе указываются все наименования территориально обособленных подразделений ОУ, в которых располагаются технические средства, участвующие в обработке персональных данных в ИСПДн, и их адреса.

19. Характеристики средств автоматизации обработки персональных данных

Характеристики средств автоматизации обработки персональных данных приведены в таблице 14.

Таблица 14. Характеристики средств автоматизации обработки персональных данных

№ п/п	Характеристика базы данных	Значение, характеризующее базу данных	Примечание
1.	Наименование средств управления базой данных	СУБД [наименование СУБД] ([наименование производителя СУБД])	
2.	Наименование специального программного обеспечения, обработки персональных данных	[наименование специального программного обеспечения ИСПДн] ([наименование производителя специального программного обеспечения ИСПДн])	
3.	Наименование базы данных	[наименование базы данных]	
4.	Адрес расположения технических средств, содержащих базу данных	[почтовый адрес и наименование (номер) помещения в котором располагаются технические средства, содержащие базу данных]	
5.	Наименование, номера (учетные, заводские, инвентарные) технических средств, содержащих базу данных	[наименование, номера (учетные, заводские, инвентарные) технических средств, содержащих базу данных]	
6.	Локальные пути доступа к файлам баз данных	[локальные пути доступа к файлам баз данных]	
7.	Формат файлов базы данных	[формат файлов базы данных, в том числе архивных]	
8.	Формат носителей архивных копий	[формат носителей архивных копий]	
9.	Места хранения архивных копий	[почтовый адрес и наименование (номер) помещения в котором хранятся архивные копии]	

Примечание: в данном разделе перечисляются все значения, характеризующее базу данных.

20. Функциональные связи информационной системы персональных данных

Наименования информационных систем персональных данных с которыми информационная система персональных данных [наименование ИСПДн] осуществляет обмен персональными данными, их расположение, наименование организаций-владельцев этих информационных систем персональных данных, а так же цель такого обмена приведены в таблице 15.

Таблица 15. Функциональные связи информационной системы персональных данных

№ п/п	Наименование ИСПДн, с которыми осуществляется взаимодействие	Расположение средств доступа к ИСПДн, с которыми осуществляется взаимодействие	Наименование организаций, владельцев ИСПДн, с которыми осуществляется взаимодействие	Цель осуществления взаимодействия между ИСПДн
1.				

Примечание: в данном разделе перечисляются:

- наименование иных информационных систем персональных данных, с которыми осуществляется взаимодействие ИСПДн;
- размещение средств доступа (взаимодействия) к иным информационным системам персональных данных;
- наименование организаций, владельцев иных информационных систем персональных данных, с которыми осуществляется взаимодействие;
- цель осуществления взаимодействия между информационными системами персональных данных.

21. Лист ознакомления

Расписка в ознакомлении с Юридическим паспортом информационной системы персональных данных [наименование ИСПДн] должностных лиц, ответственных за эксплуатацию данной информационной системы.

Таблица 16. Лист ознакомления

№ п/п	Должность	Фамилия и инициалы	Подпись
1.			

Примечание: в данном разделе указывается:

- Должности, инициалы и фамилии сотрудников, осуществляющих обработку персональных данных в информационной системе персональных данных;
- подпись указанных лиц в ознакомлении с настоящим юридическим паспортом.

Форма перечня информационных систем персональных данных

Утверждаю

И.о. ректора ОмГПУ

_____ И.М. Щеткин

«_____» _____ 20__ г.

Перечень информационных систем персональных данных
федерального государственного бюджетного образовательного учреждения высшего
профессионального образования «Омский государственный педагогический
университет»

на «_____» _____ 20__ г.

Согласовано

Первый проректор

_____ И.В. Барынькин

«_____» _____ 2010 г.

Код по номенклатуре дел:

Омск

На «___» _____ 20__ г. в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Омский государственный педагогический университет» находятся в эксплуатации следующие информационные системы персональных данных:

№ п/п	Наименование ИСПДн	Цель создания и эксплуатации ИСПДн	Перечень структурных подразделений, осуществляющих эксплуатацию ИСПДн	Структурное подразделение, ответственное за эксплуатацию ИСПДн
1.				
2.				
3.				
Итого, информационных систем персональных данных:				

Лист ознакомления руководителей структурных подразделений

№ п/п	Наименование структурного подразделения	Должность руководителя	Фамилия и инициалы	Подпись
1.				

Форма согласия на обработку персональных данных

Согласие на обработку персональных данных	
Я, _____	
(фамилия)	(имя)
(отчество)	
(основной документ, удостоверяющий личность)	(номер основного документа, удостоверяющего его личность)
(сведения о дате выдачи указанного документа)	(сведения о выдавшем указанный документ органе)
зарегистрированный по адресу: _____	
(адрес субъекта персональных данных)	
принимаю решение о предоставлении своих персональных данных в составе:	
–	
–	
(перечень персональных данных, на обработку которых дается согласие субъекта персональных данных)	
(в случае обработки специальных категорий персональных данных работника <input type="checkbox"/>)	
– сведения о состоянии здоровья работника ОУ в объеме сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции	
– сведения о состоянии здоровья учащегося ОУ в объеме сведений, которые относятся к вопросу о его обеспечении здоровья и безопасности	
(в случае обработки биометрических персональных данных)	
– личная подпись	
– фотография	
и даю согласие на их обработку включающую:	
12.	сбор персональных данных;
13.	систематизация персональных данных;
14.	накопление персональных данных;
15.	распространение персональных данных:
15.1.	передача персональных данных определенному кругу лиц (передача персональных данных);
16.	хранение персональных данных;
17.	уточнение персональных данных:
17.1.	обновление персональных данных;
17.2.	изменение персональных данных;
18.	использование персональных данных;
19.	обезличивание персональных данных;
20.	уничтожение персональных данных;
21.	блокирование персональных данных:
21.1.	временное прекращение сбор персональных данных;

21.2.	временное прекращение систематизации персональных данных;
21.3.	временное прекращение накопления персональных данных;
21.4.	временное прекращение использования персональных данных;
21.5.	временное прекращение распространения персональных данных;
21.6.	временное прекращение передачи персональных данных;
22.	снятие блокирования
<i>(перечень действий с персональными данными, на совершение которых дается согласие)</i>	
способами, определяемыми [договором, регламентом, правилами, инструкциями и положениями] (или перечислить способы обработки и в каких системах, например, «автоматизированным и исключительно автоматизированным способом в информационной системе персональных данных бухгалтерии ОУ»)	
<i>(общее описание используемых оператором способов обработки персональных данных)</i>	
своей волей и в своем интересе	
[Полное и сокращенное наименование ОУ], расположенному по адресу:	
в лице давших обязательство о неразглашении персональных данных и допущенных к обработке персональных данных для выполнения своих должностных обязанностей	
с целью:	
–	
–	
<i>(цель или цели обработки персональных данных)</i>	
(в случае обработки персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи)	
– продвижение товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи.	
(в случае обработки общедоступных персональных данных)	
– создания общедоступного источника персональных данных	
на срок: _____	
<i>(срок, в течение которого действует согласие)</i>	
Порядок отзыва согласия:	
Отзыв согласия подается в письменном виде лицом, указанным в согласии на обработку персональных данных, лично. Отзыв должен содержать:	
– номер основного документа, удостоверяющего личность субъекта персональных данных;	
– сведения о дате выдачи указанного документа и выдавшем его органе;	
– собственноручную подпись субъекта персональных данных;	
– сведения о согласии на обработку персональных данных (дата и адрес, по которому давалось согласие).	
При подаче лицом, осуществляющим прием такого отзыва, производится удостоверение личности подающего такой отзыв.	
Отзыв согласия осуществляется по адресу:	
В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных прекращение обработки персональных данных и уничтожение персональных данных будет произведено по окончании календарного года, в течении которого поступил отзыв	
Порядок защиты субъектом персональных данных своих прав и законных интересов:	
В соответствии с требованиями Федерального закона №152 от 27 июля 2006 г. «О персональных данных»	

(в случае если обязанность предоставления персональных данных установлена федеральным законом)

Юридические последствия отказа предоставить свои персональные данные, если обязанность предоставления персональных данных установлена федеральным законом:

(в случае исключительно автоматизированной обработки персональных данных)

Порядок принятия решения на основании исключительно автоматизированной обработки персональных данных субъекта персональных данных:

Возможные юридические последствия решения на основании исключительно автоматизированной обработки персональных данных субъекта персональных данных:

Порядок защиты субъектом персональных данных своих прав и законных интересов

(«я возражаю против решения исключительно автоматизированной обработки моих персональных данных» – заполняется собственноручно, в случае наличия такого возражения)

(в случае передачи персональных данных третьим лицам)

Наименование оператора, которому будут передаваться персональные данные

Адрес оператора, которому будут передаваться персональные данные

Цель передачи персональных данных

Перечень персональных данных, на передачу которых дается согласие субъекта персональных данных

Срок, в течение которого действует согласие на передачу

Для обработки персональных данных, содержащихся в согласии в письменной форме субъекта на обработку его персональных данных, дополнительного согласия не требуется (пункт 5 статья 9 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных»).

(в случае обработки общедоступных персональных данных)

Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов

(в случае трансграничной передачи персональных данных)

Наименование оператора, которому будут передаваться персональные данные

Иностранные государства, которым будут передаваться персональные данные

Цель передачи персональных данных

Перечень персональных данных, на передачу которых дается согласие субъекта персональных данных

Я подтверждаю, что предоставленные мною персональные данные являются полными, актуальными и достоверными.

Я обязуюсь своевременно извещать об изменении предоставленных персональных данных

« ____ » _____ 20 ____ г.

(личная подпись)

(инициалы,
фамилия)

Предоставленные данные соответствуют предъявленным документам, удостоверяющим личность

« ____ » _____ 20 ____ г.

(должность) (личная подпись)

(инициалы,
фамилия)

Приложение 5. Форма согласия субъекта персональных данных на запрос его персональных данных у третьих лиц

Приложение 5.

Форма согласия субъекта персональных данных на запрос его персональных данных у третьих лиц

Согласие на запрос персональных данных у третьих лиц	
Я, _____ (фамилия) (имя) (отчество)	
(основной документ, удостоверяющий личность)	(номер основного документа, удостоверяющего его личность)
(сведения о дате выдачи указанного документа)	(сведения о выдавшем указанный документ органе)
зарегистрированный по адресу: _____ (адрес субъекта персональных данных)	
своей волей и в своем интересе даю согласие (наименование оператора, которому дается согласие) (адрес оператора, которому дается согласие)	
на передачу моих персональных данных (перечень действий с персональными данными, на совершение которых дается согласие)	
в составе: — (перечень персональных данных, на обработку которых дается согласие субъекта персональных данных)	
[Полное и сокращенное наименование ОУ] (наименование оператора, которому будут передаваться персональные данные) зарегистрированному по адресу: (адрес оператора, которому будут передаваться персональные данные) с целью (цель передачи персональных данных) в срок до « _____ » _____ 20 ____ г. (срок, в течение которого действует согласие на передачу)	
посредством почтовой связи или передачи документов лично представителю ОУ (нарочному) (общее описание используемых оператором способов обработки персональных данных)	
« _____ » _____ 20 ____ г. _____ (личная подпись) (инициалы, фамилия)	

Приложение 6. Форма журнала учета лиц (организаций), получивших доступ к персональным данным, и (или) лиц (организаций), которым такая информация была предоставлена или передана

Приложение 6.

Форма журнала учета лиц (организаций), получивших доступ к персональным данным, и (или) лиц (организаций), которым такая информация была предоставлена или передана

№ п/п	Дата ознакомления	Основание на ознакомление	Лицо (организация) получившее доступ к персональным данным	С какими данными ознакомлены
1.				
2.				
3.				

Приложение 7. Форма акта уничтожения персональных данных субъектов персональных данных по достижении цели обработки, внесения изменений, блокировки и т.д.

Приложение 7.

Форма акта уничтожения персональных данных субъектов персональных данных по достижении цели обработки, внесения изменений, блокировки и т.д.

**Акт
уничтожения персональных данных**

№ _____

«___» _____ 2011 г.

Комиссия в составе:
председателя комиссии:

членов комиссии:

уничтожила персональные данные:

№ п/п	Дата уничтожения	ФИО	Основание на уничтожение
1.			
2.			
3.			
4.			
5.			

Председатель комиссии

Члены комиссии

Форма уведомлений о совершенных операциях над персональными данными

Официальный бланк ОмГПУ

Уважаемый (–ая), [Имя Отчество]!

В соответствии с требованиями Федерального закона Российской Федерации №152–ФЗ от 27 июля 2006 года «О персональных данных» уведомляем Вас

– о результатах рассмотрения возражения о принятии решения при обработке Ваших персональных данных на основании исключительно автоматизированной обработки [ответ по существу]

– о внесенных изменениях и предпринятых мерах по уничтожению или блокированию соответствующих персональных данных на основании предоставленных субъектом персональных данных сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет **ОмГПУ** являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки [ответ по существу]

– об устранении выявленных неправомерных действий с персональными данными или об уничтожении персональных данных, в случае невозможности устранения допущенных нарушений [ответ по существу]

– о прекращении обработки персональных данных и уничтожении соответствующих персональных данных в случае достижения цели обработки персональных данных [ответ по существу]

– о прекращении обработки персональных данных и уничтожении соответствующих персональных данных в случае отзыва субъектом персональных данных согласия на обработку своих персональных [ответ по существу]

– о получении Ваших персональных данных **ОмГПУ**, располагается по адресу г., ул., д. с целью [цель обработки персональных данных] на основании [правовое основание]. Обработка Ваших персональных данных будет осуществляться только специально допущенными сотрудниками ОмГПУ. В соответствии с действующим законодательством РФ в области персональных данных Вы имеете право: давать своей волей и в своем интересе и отзывать согласие на обработку своих персональных данных в предусмотренных действующим законодательством Российской Федерации случаях; на получение сведений об ОмГПУ (в объеме необходимом для защиты своих прав и законных интересов по вопросам обработки своих персональных данных), о месте нахождения ОмГПУ, о наличии у ОмГПУ своих персональных данных, а также на ознакомление с такими персональными данными; подавать запрос на доступ к своим персональным данным; требовать безвозмездного предоставления возможности ознакомления со своими персональными данными, а также внесения в них необходимых изменений, их уничтожения или блокирования при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; получать уведомления по вопросам обработки персональных данных в установленных

действующим законодательством Российской Федерации случаях и сроки; требовать от ОмГПУ разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов; обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

С Уважением,
ОмГПУ

Приложение 9. Содержание дополнений к договорам с физическими лицами по вопросам обработки персональных данных

Приложение 9.

Содержание дополнений к договорам с физическими лицами по вопросам обработки персональных данных

Должны быть отражены все вопросы, отраженные в согласии